Avira Internet Security 2012

Manuale utente

Marchio registrato e copyright

Marchio registrato

Windows è un marchio registrato di Microsoft Corporation negli Stati Uniti e in altri paesi.
Tutti gli altri marchi o nomi di prodotti sono marchi registrati del legittimo proprietario.
I marchi protetti non sono contrassegnati come tali in questo manuale. Ciò tuttavia non significa che possano essere liberamente utilizzati.

Note sul Copyright

Per Avira Internet Security 2012 viene utilizzato codice di terzi. Ringraziamo i possessori di copyright per aver messo a disposizione il proprio codice.
Informazioni dettagliate sul copyright sono disponibili nella guida del programma di Avira Internet Security 2012 in "Third Party Licenses".

Indice

1. Introduzione

Il prodotto Avira protegge efficacemente il computer da virus, worm, trojan, adware, spyware e altri pericoli. In questo manuale vengono brevemente descritti virus o malware (software dannoso) e programmi indesiderati.

La guida descrive l'installazione e il funzionamento del programma.

Sul sito Web Avira sono disponibili numerose opzioni e ulteriori informazioni:

http://www.avira.it

Sul sito Web Avira è possibile:

- richiamare informazioni su ulteriori programmi Avira Desktop
- scaricare il programma Avira Desktop più recente
- scaricare il manuale del prodotto più recente in formato PDF
- scaricare strumenti di supporto e riparazione gratuiti
- utilizzare la banca dati completa e gli articoli FAQ relativi alla risoluzione di problemi
- richiamare gli indirizzi di assistenza specifici per paese.

Il team di Avira

1.1 Simboli ed evidenziazioni

Si utilizzano i seguenti simboli:

Simbolo/Definizione	Spiegazione
✓	Esiste un requisito che deve essere soddisfatto prima che sia eseguita un'operazione.
▶	Prima di un'operazione che deve essere eseguita dall'utente.
→	Prima di un evento scaturito dall'operazione precedente.
Attenzione	Prima di un avviso di pericolo di una significativa perdita di dati.

Suggerimenti	Prima di un messaggio con informazioni particolarmente importanti o prima di un suggerimento che agevola la comprensione e l'uso del prodotto Avira.

Si utilizzano le seguenti evidenziazioni:

Evidenziazione	**Spiegazione**
Corsivo	Nome del file o percorso.
	Elementi dell'interfaccia del software che vengono visualizzati (ad esempio sezione della finestra o avviso di errore).
Grassetto	Elementi dell'interfaccia software su cui è possibile fare clic (ad esempio voci di menu, rubriche, campi di opzione o pulsanti).

2. Informazioni sul prodotto

2.1 Panoramica

In questo capitolo è possibile ricevere tutte le informazioni importanti per l'acquisto e l'utilizzo del prodotto Avira:

- vedere capitolo: Prestazioni
- vedere capitolo: Requisiti di sistema
- vedere capitolo: Licenza e aggiornamento
- vedere capitolo: Gestione delle licenze

I prodotti Avira offrono strumenti completi e flessibili per proteggere efficacemente il computer da virus, malware, programmi indesiderati e altri pericoli.

- Si noti:

Attenzione
La perdita di dati importanti ha spesso conseguenze drammatiche. Nemmeno il miglior programma antivirus può offrire una protezione al 100% contro la perdita di dati. Si consiglia di eseguire regolarmente copie di sicurezza (backup) dei dati.

Suggerimenti
Un programma in grado di proteggere il computer da virus, malware, programmi indesiderati e altri pericoli può essere affidabile ed efficace solo se aggiornato regolarmente. Si consiglia di garantire l'aggiornamento del prodotto Avira tramite aggiornamenti automatici. Configurare adeguatamente il programma.

2.2 Prestazioni

Il prodotto Avira dispone delle seguenti funzioni:

- Control Center per il monitoraggio, l'amministrazione e la gestione dell'intero programma
- Configurazione centrale con configurazione semplice in modalità esperto oppure standard e dotata di guida in linea sensibile al contesto
- System Scanner (On-Demand Scan) con scansione di tutti i tipi noti di virus e malware gestita da profilo e configurabile.

- Integrazione nella funzionalità di controllo di Windows Vista (Controllo dell'account utente) per poter eseguire operazioni per le quali sono necessari i diritti di amministratore.
- Realtime Protection (On-Access Scan) per il costante monitoraggio di tutti gli accessi ai file
- Componente ProActiv per il monitoraggio permanente di azioni eseguite dai programmi (solo per sistemi a 32 bit, non disponibile in Windows 2000)
- Mail Protection (sistema di scansione POP3, sistema di scansione IMAP e sistema di scansione SMTP) per il controllo permanente delle email per virus e malware. Verifica estesa degli allegati email
- Componente Child Protection è provvisto di filtri basati sui ruoli per filtrare pagine Web indesiderate e per limitare il tempo di utilizzo di Internet
- Componente Backup per la creazione di backup dei dati (backup speculari)
- Gestione integrata della quarantena per l'isolamento e il trattamento di file sospetti
- Rootkits Protection per il rilevamento di malware installatisi occultamente nel sistema del computer (i cosiddetti rootkit (non disponibile in Windows XP 64 Bit)
- Accesso diretto in Internet a informazioni dettagliate su virus rilevati e malware
- Aggiornamento semplice e rapido del programma, delle definizioni dei virus (VDF) e del motore di ricerca mediante Aggiornamento singolo file e aggiornamento incrementale VDF mediante un server web su Internet
- Licenza facilmente gestibile dall'utente
- integrato per la pianificazione di operazioni singole o ricorrenti come aggiornamenti o scansioni
- Identificazione estremamente precisa di virus e malware per mezzo di tecnologie di ricerca (motore di ricerca) che includono la procedura di ricerca euristica
- Identificazione di tutti i tipi di archivio convenzionali, inclusa l'identificazione di archivi nascosti e Smart-Extension
- Elevata performance grazie alla capacità multi threading (scansione contemporanea di molti file ad alta velocità)
- FireWall Avira per la protezione del computer da accessi non consentiti provenienti da Internet, da una rete o da accessi a Internet/rete da parte di utenti non autorizzati

2.3 Requisiti di sistema

È necessario soddisfare i seguenti requisiti di sistema:

- Computer a partire dal Pentium, minimo 1 GHz
- Sistema operativo
  - Windows XP, SP3 (32 o 64 Bit) o
  - Windows Vista (32 o 64 Bit, SP1 consigliato) o
  - Windows 7 (32 o 64 Bit)

- Min. 150 MB di memoria libera sull'hard disk (maggiore quantità di memoria se si utilizza la quarantena e la memoria temporanea)
- Min. 512 MB di memoria principale in Windows XP
- Min. 1024 MB di memoria principale in Windows Vista, Windows 7
- Per l'installazione del programma: diritti di amministratore
- Per tutte le installazioni: Windows Internet Explorer 6.0 o superiore
- Eventuale connessione Internet (vedi Installazione)

2.4 Licenza e aggiornamento

Per poter utilizzare il prodotto Avira è necessario possedere una licenza. In questo modo si prende visione delle condizioni di licenza.

La licenza viene assegnata sotto forma di una chiave di attivazione. La chiave di attivazione è un codice alfanumerico che l'utente riceve all'acquisto del prodotto Avira. La chiave di attivazione comprende i dati esatti della licenza, ossia quali sono i programmi dotati di licenza e per quale periodo.

Se il prodotto Avira è stato acquistato in Internet, l'utente riceverà la chiave di attivazione per email, altrimenti è riportata sulla confezione del prodotto.

Per attivare la licenza del programma, è necessario immettere tale chiave durante l'attivazione del programma. L'attivazione del prodotto può avvenire durante l'installazione. Tuttavia, è possibile attivare il prodotto Avira anche in seguito nel Sistema di gestione delle licenze in Guida in linea > Sistema di gestione delle licenze.

Nel Sistema di gestione delle licenze è possibile avviare un aggiornamento a un prodotto della famiglia Avira Desktop: In questo modo non è necessario disinstallare il vecchio prodotto manualmente e installare manualmente il nuovo. Tramite l'aggiornamento dal Sistema di gestione delle licenze immettere nell'apposito campo la chiave di attivazione del prodotto di cui si desidera effettuare l'aggiornamento. Il nuovo prodotto viene installato automaticamente.

Per raggiungere alta affidabilità e sicurezza per il computer, Avira rammenta all'utente di eseguire l'aggiornamento all'ultima versione. Fare clic su **Upgrade** nell'elemento pop-up per la migrazione all'ultima versione e l'utente verrà inoltrato alla pagina di aggiornamento specifica del prodotto. È possibile eseguire un aggiornamento per il prodotto attuale o acquistare un prodotto dall'ampia gamma di prodotti Avira. La pagina panoramica dei prodotti Avira mostra quale prodotto viene utilizzato attualmente e offre la possibilità di confrontarlo con altri prodotti Avira. Per ulteriori informazioni, fare clic sul simbolo delle informazioni a destra accanto al nome del prodotto. Se si desidera continuare ad usare il prodotto utilizzato finora, fare clic su **Upgrade** per installare subito l'ultima versione con le funzioni migliorate. Se si desidera acquistare un prodotto dell'ampia gamma, fare clic su **Acquista** in fondo alla colonna del prodotto corrispondente. Si viene reindirizzati al Negozio online di Avira per eseguire l'ordinazione.

Suggerimenti
A seconda del prodotto e del sistema operativo, è necessario possedere eventualmente i diritti di amministratore per eseguire l'aggiornamento. Registrarsi come amministratore e installare l'ultima versione.

È possibile effettuare l'aggiornamento dei seguenti prodotti:

- Aggiornamento di Avira AntiVir Personal ad Avira Free Antivirus.
- Aggiornamento di Avira AntiVir Personal ad Avira Antivirus Premium 2012.
- Aggiornamento da Avira AntiVir Premium ad Avira Internet Security 2012.
- Aggiornamento da Avira AntiVir Premium Security Suite ad Avira Professional Security.

2.4.1 Sistema di gestione delle licenze

IlAvira Internet Security 2012 sistema di gestione delle licenze permette un'installazione molto semplice dellaAvira Internet Security 2012 licenza.

Avira Internet Security 2012 Sistema di gestione delle licenze

È possibile effettuare l'installazione della licenza selezionandola con un doppio clic nel Filemanager o nell'email di attivazione e seguendo le istruzioni delle schermate.

Suggerimenti
IlAvira Internet Security 2012 sistema di gestione delle licenze copia automaticamente la licenza nella cartella del prodotto. Se è già disponibile una licenza, appare una nota che chiede se il file di licenza deve essere sostituito. Il file esistente viene sovrascritto con l'attuale file di licenza.

3. Installazione e disinstallazione

3.1 Panoramica

In questo capitolo si ottengono informazioni relative all'installazione e la disinstallazione del prodotto Avira:

- vedere capitolo: Prima dell'installazione premesse, preparazione del computer all'installazione
- vedere capitolo: Installazione Express: installazione standard in base alle impostazioni predefinite
- vedere capitolo: Installazione personalizzata: installazione configurabile
- vedere capitolo: Installazione prodotto di prova
- vedere capitolo: Assistente di configurazione
- vedere capitolo: Modifiche all'installazione
- vedere capitolo: Moduli di installazione
- vedere capitolo: Disinstallazione: esegui disinstallazione

3.1.1 Modi di installazione

Durante l'installazione mediante l'assistente di installazione è possibile selezionare un tipo di setup:

Express

- Installazione dei componenti standard in corso...
- I file del programma vengono installati in una directory standard predefinita in *C:\Programmi*.
- Il prodotto Avira verrà installato con le impostazioni standard. È possibile effettuare impostazioni predefinite nell'assistente di configurazione.

Personalizzata

- È possibile selezionare per l'installazione singoli componenti del programma (vedere capitolo Installazione e disinstallazione > Moduli di installazione).
- Si può scegliere una cartella di destinazione per i file di programma da installare.
- È possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu di avvio.
- Con la configurazione guidata è possibile effettuare impostazioni personalizzate del prodotto Avira e indurre una breve scansione del sistema direttamente dopo l'installazione.

3.2 Prima dell'installazione

Suggerimenti
Prima dell'installazione verificare che il computer soddisfi i requisiti di sistema.
Se il computer soddisfa tutti i requisiti minimi, è possibile installare il prodotto Avira.

Suggerimenti
Nell'installazione su un sistema operativo server, Realtime Protection e Protezione file non sono disponibili.

Inizializzazione prima dell'installazione

✓ Chiudere il programma email. Si consiglia inoltre di chiudere tutte le applicazioni in uso.
✓ Assicurarsi che non siano installate altre protezioni contro virus. Le funzioni automatiche di protezione di diverse applicazioni antivirus potrebbero entrare in conflitto.

↳ Il prodotto Avira scansionerà il computer per controllare l'eventuale presenza di software incompatibili.

↳ In caso di rilevamento di software incompatibile viene generato un elenco corrispondete di questi programmi.

↳ Si consiglia di disinstallare il software che espone a rischi la sicurezza del computer.

- Scegliere dall'elenco quei programmi, che devono essere eliminati dal computer automaticamente, quindi fare clic su **Continua**.
- Alcuni programmi possono essere eliminati dal computer solo manualmente. Selezionare i programmi e fare clic su **Continua**.

↳ La disinstallazione di uno o più programmi richiede il riavvio del computer. Dopo il riavvio, l'installazione continua.

Attenzione
Finché la procedura di installazione del prodotto Avira non è conclusa, il computer non è protetto.

Installazione

Il programma di installazione funziona in modalità di dialogo. Nella maggior parte dei passaggi di installazione è sufficiente fare un semplice clic per continuare.

I pulsanti principali hanno le seguenti funzioni:

- **OK**: per confermare l'azione.
- **Annulla**: per annullare l'azione.
- **Continua**: per passare alla fase successiva.
- **Indietro**: per passare alla fase precedente.

▸ Stabilire una connessione Internet. La connessione a Internet è necessaria per eseguire i seguenti passaggi dell'installazione:

  - Scaricare i file attuali di programma e del motore di ricerca, nonché i file di definizione dei virus aggiornati mediante il programma di installazione (per installazione basata su Internet)
  - Attivazione del programma
  - Esecuzione di un eventuale aggiornamento a installazione conclusa

▸ Tenere a portata di mano la chiave di licenza del prodotto Avira, se si desidera attivarlo.

Suggerimenti
Installazione basata su Internet:
per eseguire un'installazione basata su Internet del programma, è disponibile un programma di installazione che carica i file di programma aggiornati prima di eseguire l'installazione dai server Web di Avira. Tale procedura garantisce l'installazione di prodotto Avira con un file di definizione dei virus aggiornato.

Installazione con un pacchetto di installazione:
il pacchetto di installazione contiene sia il programma di installazione sia tutti i file di programma necessari. Tuttavia nell'installazione con un pacchetto di installazione non è possibile effettuare la selezione della lingua per il prodotto Avira. Al termine dell'installazione si consiglia di eseguire un aggiornamento del file di definizione dei virus.

Suggerimenti
Per attivare il prodotto, il prodotto Avira comunica tramite il protocollo HTTP e la porta 80 (comunicazione Web), nonché tramite il protocollo di codifica SSL e la porta 443 con i server di Avira. Se si utilizza un firewall, assicurarsi che la connessione necessaria e i dati in entrata e in uscita non vengano bloccati dal firewall.

3.3 Installazione Express

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

↳ Appare la finestra di dialogo **Benvenuti**.

- Fare clic su **Avanti** per continuare l'installazione.

↳ Appare la finestra di dialogo **Seleziona lingua**.

- Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Installazione con un pacchetto di installazione

↳ Viene visualizzata la finestra **Preparazione dell'installazione in corso**.

↳ Il file di installazione viene decompresso. La routine di installazione viene avviata.

↳ Appare la finestra di dialogo**Selezionare modalità di installazione**.

> **Suggerimenti**
> L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è preimpostata come default. Per eseguire una **installazione personalizzata**, continuare a leggere qui di seguito: Installazione > Installazione personalizzata.

- È possibile partecipare alla community di Avira ProActiv (Configurazione > Realtime Protection > ProActiv).
- Confermare **l'accettazione dei termini del contratto di licenza con l'utente finale**. Se si desidera leggere i dettagli dei contratti di licen, fare clic sul link corrispondente.
- Fare clic su **Avanti**.
- Se si ha acconsentito a partecipare alla community Avira ProActiv, aprire la finestra informativa di **ProActiv Community**, in cui si possono reperire altre informazioni sulla verifica online.
- Fare clic su **Avanti**.

↳ L'*assistente per l'installazione della licenza* si apre e aiuta l'utente nell'attivazione del programma.

↳ A questo punto si ha la possibilità di configurare un server proxy.

Fare clic su **Impostazioni proxy** per configurare il server proxy e confermare le impostazioni con **OK**.

↳ Se è già stato ricevuto un codice di attivazione, selezionare **Attiva il prodotto**.

In alternativa, fare clic sul link **Ho già un file di licenza HBEDV.KEY valido**.

- Nella finestra **Apri file** selezionare il file *HBEDV.KEY* e fare clic su **Apri**.

↳ Il codice di attivazione viene copiato nell'assistente per l'installazione della licenza.

- Se si desidera provare il prodotto, consultare il capitolo Installazione prodotto di prova, più avanti.

↳ L'avanzamento dell'installazione viene visualizzato tramite una barra verde.

↳ Fare clic su **Fine** per terminare il setup e uscire dal programma di installazione.

↳ L'Icona Tray di Avira si trova nella barra delle applicazioni.

↳ Il modulo **Updater** ricerca gli eventuali aggiornamenti disponibili per proteggere in modo ottimale il computer.

↳ La finestra sullo stato di**Luke Filewalker** si apre con una prima ricerca diretta del sistema di scansione e informa l'utente circa lo stato della scansione visualizzandone i risultati.

- Se dopo la scansione del sistema viene richiesto di riavviare il sistema, eseguire tale operazione per consentire la protezione completa del sistema stesso.

Se l'installazione è avvenuta con successo, si consiglia di verificare lo stato di aggiornamento del programma di protezione nella sezione **Stato** del Control Center.

- Se il prodotto Avira visualizza un messaggio ad indicare che il computer non è completamente protetto, fare clic su **Risoluzione del problema**.

↳ Compare la finestra di dialogo **Ripristina la protezione**.

- Massimizzare la sicurezza del sistema in uso attivando le opzioni prestabilite.
- Infine, è possibile eventualmente eseguire una scansione completa del sistema.

3.4 Installazione personalizzata

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

↳ Appare la finestra di dialogo **Benvenuti**.

- Fare clic su **Avanti** per continuare l'installazione.

↳ Appare la finestra di dialogo **Seleziona lingua**.

- Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Installazione con un pacchetto di installazione

↳ Viene visualizzata la finestra **Preparazione dell'installazione in corso**.

↳ Il file di installazione viene decompresso. La routine di installazione viene avviata.

↳ Appare la finestra di dialogo**Selezionare modalità di installazione**.

> **Suggerimenti**
> L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è preimpostata come default. Se si desidera eseguire tale operazione, continuare a leggere qui di seguito: Installazione > Installazione Express.

- Come modalità di installazione desiderata selezionare **Personalizzata**.
- Confermare **l'accettazione dei termini del contratto di licenza con l'utente finale**. Se si desidera leggere i dettagli dei contratti di licen, fare clic sul link corrispondente.
- Fare clic su **Avanti**.

  ↳ Viene visualizzata la finestra **Seleziona directory di destinazione**.

  ↳ La directory preimpostata è *C:\Programmi\Avira\AntiVir Desktop*
- Fare clic su **Avanti** per continuare con l'installazione.

  \- OPPURE -

  Selezionare mediante **Sfoglia** un'altra directory di destinazione e confermare con **Avanti**.

  ↳ Appare la finestra **Installa i componenti**:
- Attivare o disattivare i componenti desiderati e confermare con **Avanti**.

  ↳ Se si sono selezionati i componenti ProActiv per l'installazione, compare la finestra **Community Avira ProActiv**.
  Si ha quindi la possibilità di confermare la propria partecipazione alla community Avira ProActiv: se l'opzione è attivata, Avira ProActiv invia i dati relativi ai programmi sospetti, indicati dai componenti ProActiv, ad Avira Malware Research Center. I dati vengono impiegati unicamente per una più ampia verifica online e per l'ampliamento e il perfezionamento della tecnologia di riconoscimento. Mediante il link **ulteriori informazioni** è possibile richiamare i dettagli della verifica online.
- Se viene visualizzata la finestra **Community Avira ProActiv**, attivare o disattivare la partecipazione alla community Avira ProActiv e confermare con **Avanti**.

↳ Nelle seguenti finestre di dialogo è possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu.

- Fare clic su **Avanti**.

↳ Si apre l'assistente per l'installazione della licenza.

Per attivare il programma, sono disponibili le seguenti opzioni:

- Immissione di una chiave di attivazione
  Immettendo la chiave di attivazione, il prodotto Avira verrà attivato con la licenza dell'utente.
- Scelta dell'opzione **Prova il prodotto**
  Selezionando **Prova il prodotto**, durante la procedura di attivazione verrà generata una licenza di prova con cui viene attivato il programma. È possibile provare il prodotto Avira per un periodo di tempo determinato in tutte le sue funzioni (vedere Installazione prodotto di prova).

Suggerimento
Tramite l'opzione **File di licenza valido hbedv.key disponibile**, è possibile leggere un file di licenza valido. Il file di licenza viene generato durante la procedura di attivazione del prodotto tramite una chiave di attivazione valida e archiviato nella directory del prodotto Avira in uso. Utilizzare questa opzione se si è già eseguita l'attivazione del prodotto e si desidera installare nuovamente il prodotto Avira.

Suggerimenti
In alcune versioni in vendita dei prodotti Avira, la chiave di attivazione è già memorizzata nel prodotto stesso. Pertanto non è necessario immettere una chiave di attivazione. In alcuni casi la chiave di attivazione memorizzata viene visualizzata nell'assistente.

Suggerimenti
Per attivare il programma, viene stabilita una connessione ai server di Avira. In **Impostazioni proxy** è possibile configurare la connessione Internet tramite un server proxy.

- Selezionare una procedura di attivazione e confermarla con **Avanti**

Attivazione del prodotto

↳ Viene aperta una finestra di dialogo in cui immettere i propri dati personali.

- Immettere i propri dati e fare clic su **Avanti.**

↳ I dati vengono trasferiti e controllati sui server di Avira. Il prodotto Avira verrà attivato con la licenza dell'utente.

↳ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente.

- Fare clic su **Avanti**.
- Saltare la sezione seguente "Attivazione tramite la selezione dell'opzione **hbedv.key valido disponibile**".

Selezione dell'opzione "hbedv.key valido disponibile"

↳ Viene aperta una finestra di dialogo per la lettura del file di licenza.

- Selezionare il file di licenza *hbedv.key* con i dati di licenza dell'utente per il programma e fare clic su **Apri**.

↳ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente.

- Fare clic su **Avanti**.

Prosecuzione dopo la conclusione dell'attivazione o il caricamento del file di licenza

Nell'assistente per l'installazione della licenza è possibile registrarsi come cliente e abbonarsi alla *newsletter di Avira*. A tal fine è necessario immettere i propri dati personali.

- Inserire eventualmente i propri dati e confermarli con **Avanti**.

↳ Durante la registrazione, nella seguente finestra di dialogo viene visualizzato il risultato dell'attivazione.

- Fare clic su **Avanti**.

↳ I componenti del programma vengono installati. L'avanzamento dell'installazione viene visualizzato nella finestra di dialogo.

- Dopo la chiusura del processo di installazione, terminare quest'ultima con **Fine**.

↳ Si chiude l'assistente di installazione e si apre l'Assistente di configurazione.

3.5 Installazione prodotto di prova

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

↳ Appare la finestra di dialogo **Benvenuti**.

- Fare clic su **Avanti** per continuare l'installazione.

↳ Appare la finestra di dialogo **Seleziona lingua**.

- Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

  ↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Suggerimenti
L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è preimpostata come default. Per eseguire una *installazione personalizzata*, continuare a leggere qui di seguito: Installazione > Installazione personalizzata.

- È possibile partecipare alla community di Avira ProActiv (Configurazione > Realtime Protection > ProActiv).
- Confermare **l'accettazione dei termini del contratto di licenza con l'utente finale**. Se si desidera leggere i dettagli dei contratti di licenza, fare clic sul link relativo.
- Fare clic su **Avanti**.
- Se si ha acconsentito a partecipare alla community Avira ProActiv, aprire la finestra informativa di **ProActiv Community**, in cui si possono reperire altre informazioni sulla verifica online.
- Fare clic su **Avanti**.

  ↳ Si aprel' *assistente per l'installazione della licenza*, con il cui aiuto è possibile attivare il prodotto.

  ↳ L'assistente offre anche la possibilità di definire un server proxy.

- Fare clic su **Impostazioni proxy** per effettuare la configurazione necessaria e confermare con **OK**.
- Selezionare nell'assistente per l'installazione della licenza **Prova il prodotto** e fare clic su **Continua**.
- Immettere i propri dati nei campi obbligatori della registrazione. Decidere se si desidera abbonarsi alla *newsletter di Avira* e fare clic su **Avanti**.

  ↳ L'avanzamento dell'installazione viene visualizzato tramite una barra verde.

- Fare clic su **Fine** per terminare l'installazione e chiudere l'assistente per l'installazione della licenza.
- Viene richiesto di eseguire un riavvio per attivare il prodotto Avira. Fare clic su **Sì** per avviare un riavvio immediato.

  ↳ L'Icona Tray di Avira è inserita nella barra delle applicazioni.

  ↳ La licenza di prova ha una validità di 31 giorni.

3.6 Assistente di configurazione

Nell'installazione personalizzata, alla fine si apre l'assistente di configurazione. Quest'ultimo permette di effettuare importanti impostazioni predefinite per il prodotto Avira.

- Fare clic su **Avanti** nella finestra di benvenuto dell'assistente di configurazione per iniziare la configurazione del programma.
  - ↳ Nella finestra di dialogo **Configura AHeAD** è possibile selezionare un livello di riconoscimento per la tecnologia AHeAD. Il livello di riconoscimento selezionato viene registrato per l'impostazione della tecnologia AHeAD di System Scanner (scansione diretta) e di Realtime Protection (scansione in tempo reale).
- Selezionare un livello di riconoscimento e proseguire la configurazione con **Avanti**.
  - ↳ Nella finestra di dialogo seguente **Seleziona categorie estese delle minacce** è possibile adattare le funzioni di protezione del proprio prodotto Avira con la selezione delle categorie delle minacce.
- Attivare eventualmente ulteriori categorie delle minacce e proseguire la configurazione con **Avanti**.
  - ↳ Nel caso in cui si sia selezionato il modulo di installazione Avira FireWall, compare la finestra di dialogo **Regole standard per l'accesso alla rete e l'utilizzo delle risorse di rete**. È possibile decidere se Avira Firewall può autorizzare l'accesso esterno a risorse condivise nonché l'accesso alla rete di applicazioni di produttori affidabili.
- Attivare le opzioni desiderate e proseguire la configurazione con **Avanti**.
  - ↳ Nel caso in cui si sia selezionato il modulo di installazione Avira Realtime Protection, compare la finestra di dialogo **Modalità di avvio di Realtime Protection**. È ora possibile stabilire il momento in cui avviare Realtime Protection. Nella modalità di avvio indicata, Realtime Protection viene avviato a ogni riavvio del computer.

Suggerimenti
La modalità di avvio indicata di Realtime Protection viene memorizzata nel registro e non può essere modificata mediante la configurazione.

Suggerimenti
Al momento dell'avvio del computer, un'eventuale conseguenza della selezione della modalità di avvio di default per Realtime Protection (avvio normale) e di un rapido accesso all'account utente può essere la mancata scansione dei programmi che si avviano automaticamente all'avvio del sistema, dal momento che essi vengono avviati prima del completo caricamento di Realtime Protection.

- Attivare l'opzione desiderata e proseguire la configurazione con **Avanti**.

↳ Nel caso in cui si sia selezionato il modulo di installazione Avira Web Protection, compare la finestra di dialogo **Attiva protezione bambini**. È possibile assegnare diversi ruoli per l'uso di Internet a seconda degli utenti del calcolatore, bambino, adolescente e adulto. Il servizio Protezione bambini può anche essere disattivato.

- Attivare le opzioni desiderate per la protezione bambini e proseguire la configurazione con **Avanti**.

↳ Nella finestra di dialogo seguente **Inserisci password**, è possibile proteggere l'accesso alla configurazione con una password. Questa opzione è particolarmente consigliata quando è attiva la protezione bambini.

↳ Nella finestra di dialogo seguente **Scansione del sistema** è possibile attivare o disattivare l'esecuzione di una scansione rapida del sistema. La scansione rapida del sistema viene eseguita al termine della configurazione e prima di riavviare il computer, e verifica la presenza di virus e malware nei programmi avviati e nei file di sistema più importanti.

- Attivare o disattivare l'opzione **Scansione rapida del sistema** e proseguire la configurazione con **Avanti**.

↳ Nella finestra di dialogo seguente è possibile terminare la configurazione con **Fine**.

↳ Le impostazioni indicate e selezionate vengono registrate.

↳ Se è attivata l'opzione **Scansione rapida del sistema**, si apre la finestra **Luke Filewalker**. System Scanner esegue una scansione rapida del sistema.

↳ Se dopo la scansione del sistema viene richiesto di riavviare il sistema, eseguire tale operazione per consentire la protezione completa del sistema stesso.

Se l'installazione è avvenuta con successo, si consiglia di verificare lo stato di aggiornamento del programma di protezione nella sezione **Stato** del Control Center.

- Se il prodotto Avira visualizza un messaggio ad indicare che il computer non è completamente protetto, fare clic su **Risoluzione del problema**.

↳ Compare la finestra di dialogo **Ripristina la protezione**.

- Massimizzare la sicurezza del sistema in uso attivando le opzioni prestabilite.
- Infine, è possibile eventualmente eseguire una scansione completa del sistema.

3.7 Modifiche all'installazione

È possibile aggiungere o eliminare singoli componenti del programma all'attuale installazione del prodotto Avira (vedere Capitolo Installazione e disinstallazione > Moduli d'installazione)

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **pannello di controllo di Windows**.

Selezionare il prodotto Avira desiderato e fare clic su **Modifica**. Nella finestra di dialogo di *benvenuto* del programma selezionare l'opzione **Modifica programma**. Si è così inseriti nella modifica dell'installazione.

3.8 Moduli di installazione

Nel caso di un'installazione personalizzata o di una modifica di un'installazione è possibile selezionare, aggiungere o eliminare i seguenti moduli:

- **Avira Internet Security 2012**
  Questo modulo contiene tutti i componenti necessari per l'installazione corretta del prodotto Avira.
- **Avira Realtime Protection**
  Realtime Protection di Avira è in esecuzione in background. Monitora e ripara i file, quando possibile, durante operazioni come apertura, scrittura e copia in tempo reale (On-Access = all'accesso). Se un utente esegue un'operazione (caricamento, esecuzione, copia di un file), il prodotto Avira scansiona automaticamente il file. Durante l'operazione di rinomina del file Realtime Protection di Avira non esegue alcuna scansione.
- **Avira ProActiv**
  Il componente ProActiv monitorizza le azioni delle applicazioni e ne notifica i comportamenti sospetti. Grazie a questo riconoscimento basato sul comportamento è possibile proteggersi dai malware. Il componente ProActiv è integrato in Realtime Protection di Avira.
- **Avira Mail Protection**
  Mail Protection è l'interfaccia tra il computer e il server email da cui il programma email (client email) scarica le email. Mail Protection funge da cosiddetto proxy tra il programma email e il server email. Tutte le email in entrata vengono convogliate mediante questo proxy, e, una volta ricercati virus e programmi indesiderati, vengono inoltrate al programma di email. In base alla configurazione il programma tratta le email infette automaticamente o chiede all'utente l'azione da eseguire. Inoltre, Mail Protection offre una protezione affidabile contro lo spam.
- **Avira Web Protection**
  Durante la navigazione in Internet si richiedono dati da un server Web mediante il browser Web. I dati trasferiti dal server Web (file HTML, file di script e immagini, file flash, file audio e video, ecc.) normalmente passano dalla cache del browser direttamente all'esecuzione nel browser Web cosicché non è possibile una scansione in tempo reale come quella prevista da Avira Realtime Protection. In questo modo virus e programmi indesiderati potrebbero entrare nel computer. Web Protection è un cosiddetto proxy HTTP che monitora le porte utilizzate per il trasferimento dei dati (80, 8080, 3128) e controlla la presenza di virus e programmi indesiderati nei file trasferiti. In base alla configurazione il programma tratta i file infetti automaticamente o chiede all'utente l'azione da eseguire.
- **Avira FireWall**
  Avira FireWall controlla le vie di comunicazione da e verso il computer. Consente o nega la comunicazione sulla base delle direttive di sicurezza.

- **Avira Rootkits Protection**
  Avira Rootkits Protection controlla se sul computer sono già installati programmi software che dopo l'intrusione nel computer non si riesce a rilevare con i metodi convenzionali del riconoscimento di malware.
- **Shell Extension**
  L'estensione shell crea nel menu contestuale di Windows Explorer (tasto destro del mouse) la voce *Controlla i file selezionati con Avira*. Con questa voce è possibile scansionare direttamente singoli file o directory.
- **Backup**
  Il componente Backup consente di creare manualmente e in modo automatico backup speculari dei dati.

3.9 Disinstallazione

Se si desidera eliminare il prodotto Avira dal proprio computer, è possibile utilizzare l'opzione **Software** per cambiare o rimuovere i programmi (**Cambia/Rimuovi**) nel pannello di controllo di Windows.

È possibile disinstallare il prodotto Avira (descritto ad esempio per Windows XP e Windows Vista) nel seguente modo:

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.
- Fare doppio clic su **Programmi** (Windows XP: **Software**).
- Selezionare il prodotto Avira desiderato dall'elenco e fare clic su **Rimuovi/Disinstalla**.
  - ↳ Verrà chiesto all'utente se desidera davvero eliminare il programma.
- Confermare con **Sì**.
  - ↳ All'utente viene chiesto se deve essere riattivato il firewall di Windows (dal momento che Avira FireWall viene disattivato).
- Confermare con **Sì**.
  - ↳ Tutte le componenti del programma vengono eliminate.
- Fare clic su **Fine** per terminare la disinstallazione.
  - ↳ Appare una finestra di dialogo con il suggerimento di riavviare il computer.
- Confermare con **Sì**.
  - ↳ Il prodotto Avira viene quindi disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

4. Panoramica

In questo capitolo è possibile consultare una panoramica delle funzionalità e del funzionamento del prodotto Avira.

- vedere capitolo Interfaccia e funzionamento
- vedere capitolo Come procedere

4.1 Interfaccia utente e funzionamento

È possibile usare il prodotto Avira mediante tre elementi dell'interfaccia del programma:

- Control Center: monitoraggio e gestione del prodotto Avira
- Configurazione: configurazione del prodotto Avira
- Icona Tray della barra delle applicazioni: Apertura di Control Center e altre funzioni

4.1.1 Control Center

Il Control Center serve per il monitoraggio dello stato di protezione del computer e per la gestione e il funzionamento delle componenti di protezione e delle funzioni del prodotto Avira.

La finestra del Control Center è divisa in tre sezioni: l'**elenco menu**, la **barra di navigazione** e la finestra per i dettagli **Stato**:

- **Elenco menu:** nei menu del Control Center è possibile richiamare funzioni generali del programma e informazioni sul prodotto.
- **Sezione di navigazione:** nella sezione di navigazione è possibile passare in modo semplice da una rubrica all'altra del Control Center. Le singole rubriche contengono informazioni e funzioni delle componenti del programma e sono presenti sulla barra di navigazione in base alle sezioni dei task. Esempio: sezione dei task **Sicurezza del computer** - Rubrica **Realtime Protection**.
- **Stato:** La schermata di avvio Stato consente in modo immediato di verificare se il computer è sufficientemente protetto e di avere una panoramica dei moduli attivi e del momento in cui sono stati eseguiti l'ultimo backup e l'ultima scansione di sistema. Nella finestra **Stato** si trovano i pulsanti per l'esecuzione di funzioni o azioni, come ad esempio l'attivazione o la disattivazione del servizio Child Protection.

Avvio e chiusura di Control Center

Per avviare Control Center è possibile scegliere tra le seguenti modalità:

- fare doppio clic sull'icona del programma sul desktop
- mediante la voce nel menu **Start > Programmi**.
- mediante l'Icona Tray del prodotto Avira

Si può chiudere il Control Center mediante il comando **Chiudi** nel menu **File**, con la shortcut **Alt+F4** o facendo clic sulla x nella finestra di Control Center.

Utilizzo di Control Center

Come navigare nel Control Center:

- Nella barra di navigazione fare clic su una sezione dei task sotto una rubrica.
  - ↳ La sezione dei task viene visualizzata nella finestra per i dettagli con ulteriori possibilità relative a funzionalità e configurazioni.
- Fare clic su un'altra sezione dei task per visualizzarla nella finestra per i dettagli.

> **Suggerimenti**
> Attivare la navigazione da tastiera nell'elenco menu con l'ausilio del tasto [**Alt**]. Con il tasto **Invio** si attiva la voce di menu selezionata in quel momento.
> Per aprire, chiudere o navigare nei menu del Control Center, è possibile utilizzare anche le combinazioni di tasti: tasto [**Alt**] + lettera sottolineata nel menu o nel comando. Tenere premuto il tasto [**Alt**] se si desidera richiamare un comando o un sottomenu dal menu.

Come elaborare dati o oggetti che vengono visualizzati nella finestra dei dettagli:

- Evidenziare i dati o gli oggetti che si desidera elaborare.

  Per evidenziare più elementi, tenere premuto il tasto **Ctrl** o il tasto **Shift** (selezione di elementi consecutivi) durante la selezione degli elementi.
- Fare clic sui pulsanti desiderati nella barra superiore della finestra dei dettagli per elaborare l'oggetto.

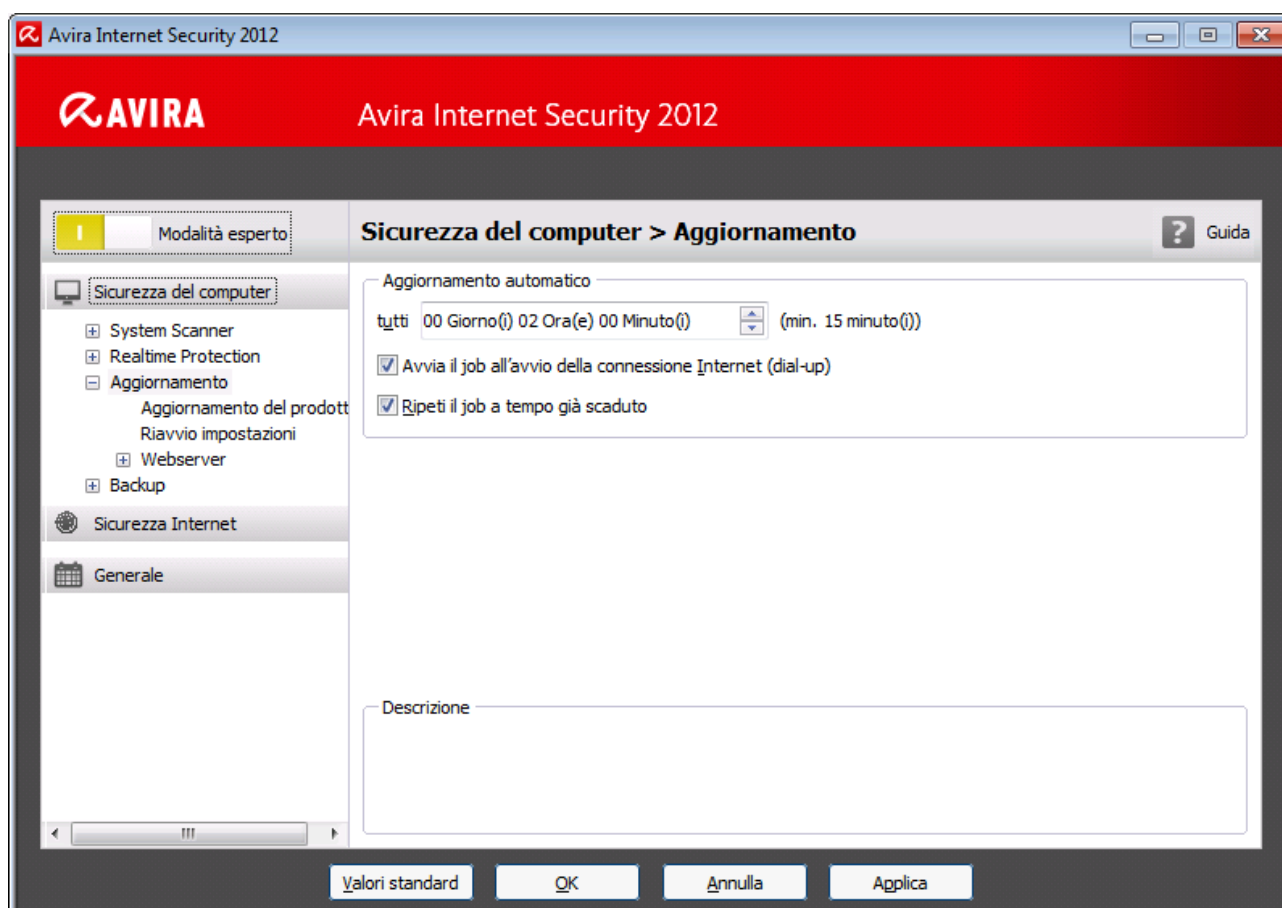
Control Center in sintesi

- **Stato**: nella schermata di avvio **Stato** sono disponibili tutte le rubriche che consentono di monitorare le funzionalità del prodotto Avira.
  - La finestra **Stato** offre la possibilità di visualizzare immediatamente quali moduli del programma sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato.Inoltre, è possibile verificare se si possiede una licenza valida.
- **Sicurezza del computer**: in **Sicurezza del computer** sono disponibili i componenti con cui eseguire la ricerca di virus e malware nei file del computer.
  - La rubrica System Scanner offre la possibilità di configurare o avviare la scansione diretta in modo semplice. I profili predefiniti consentono una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (non viene memorizzata) o con la creazione di un profilo definito dall'utente, è possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.
  - La rubrica Realtime Protection visualizza informazioni su file scansionati, così come ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e

permette il richiamo del file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili "premendo un pulsante".

- **Sicurezza Internet**: in **Sicurezza Internet** sono disponibili i componenti che consentono di proteggere il computer da virus e malware provenienti da Internet, nonché da accessi di rete indesiderati.
  - La rubrica Mail Protection mostra le email verificate, le relative proprietà e altri dati statistici. Inoltre, si ha la possibilità di spostare il filtro AntiSpam ed escludere indirizzi email dalla scansione per malware o spam. Le email possono essere eliminate anche dalla memoria temporanea di Mail Protection.
  - La rubrica Web Protection visualizza informazioni sugli URL scansionati e sui virus individuati, nonché ulteriori dati statistici che possono essere ripristinati in qualsiasi momento, e consente di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili "premendo un pulsante".
  - La rubrica FireWall offre la possibilità di configurare le impostazioni di base di Avira FireWall. Vengono inoltre visualizzate le attuali velocità di trasferimento dati e tutte le applicazioni attive che utilizzano un collegamento alla rete.
- **Gestione**: in **Gestione** sono disponibili gli strumenti che consentono di isolare e gestire file sospetti o infetti, nonché di pianificare attività ricorrenti.
  - Nella rubrica Quarantena è disponibile il cosiddetto Gestore della quarantena: la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena. Inoltre esiste la possibilità di inviare un file selezionato per email all'Avira Malware Research Center.
  - La rubrica Scheduler offre la possibilità di creare sia job temporizzati di controllo e di aggiornamento che job di backup, nonché di cancellare o modificare job esistenti.
  - La rubrica Report consente di visualizzare i risultati delle azioni eseguite.
  - La rubrica Eventi consente di ottenere informazioni sugli eventi generati dai moduli del programma.
- **Strumenti**: in **Strumenti** sono disponibili ulteriori strumenti per la sicurezza dei dati.
  - Nella rubrica Backup è possibile creare in modo semplice e rapido i backup dei dati e assegnare i job di backup.

4.1.2 Configurazione

In Configurazione è possibile effettuare le impostazioni per il prodotto Avira. Dopo l'installazione, il prodotto Avira è configurato con le impostazioni standard che assicurano la protezione ottimale del computer. Ciononostante, il computer o le richieste dell'utente per il prodotto Avira possono possedere caratteristiche particolari e richiedere un adattamento delle componenti di protezione del programma.

La configurazione dispone di una finestra di dialogo: con il pulsante **OK** o **Applica** si memorizzano le impostazioni scelte durante la configurazione, con **Annulla** si rifiutano le impostazioni, con il pulsante **Valori standard** è possibile ripristinare le impostazioni dei valori standard della configurazione. Nella barra di navigazione a sinistra è possibile selezionare singole rubriche di configurazione.

Richiamo della Configurazione

Esistono diverse possibilità per richiamare la configurazione:

- Mediante il Pannello di controllo di Windows.
- Mediante il centro sicurezza di Windows - a partire da Windows XP Service Pack 2.
- mediante l'Icona Tray del programma Avira.
- nel Control Center mediante la voce di menu Extra > Configurazione.
- Nel Control Center mediante il pulsante Configurazione.

Suggerimenti
Se si richiama la configurazione con il pulsante **Configurazione** in Control Center, si giunge nel registro di configurazione della categoria attiva in Control Center. Per selezionare un singolo registro di configurazione, è necessario

attivare la **Modalità esperto** della configurazione. In questo caso appare una finestra di dialogo, in cui viene richiesto di attivare la **Modalità esperto**.

Utilizzo della Configurazione

All'interno della finestra di configurazione si può navigare come in Esplora risorse di Windows:

- Fare clic su una voce della struttura ad albero per visualizzare questa categoria di configurazione nella finestra dei dettagli.
- Fare clic sul segno + prima delle voci per estendere la categoria di configurazione e visualizzare le rubriche di configurazione subordinate nella struttura ad albero.
- Per nascondere le rubriche di configurazione subordinate, fare clic sul segno - (meno) prima della categoria di configurazione estesa.

Suggerimenti
Per attivare o disattivare le opzioni nella configurazione e per premere i pulsanti è possibile utilizzare anche le seguenti combinazioni di tasti: tasto [**Alt**] + lettera sottolineata nei nomi opzione o nella definizione pulsanti.

Suggerimenti
Le rubriche di configurazione vengono visualizzate per intero nella modalità esperto. Attivare la **Modalità esperto** per visualizzare tutte le rubriche di configurazione. La **Modalità esperto** può essere protetta con una password da digitare al momento dell'attivazione.

Se si desidera registrare le impostazioni nella configurazione:

- Fare clic sul pulsante **OK**.

  ↬ La finestra di configurazione viene chiusa e le impostazioni registrate.

  \- OPPURE -

  Fare clic sul pulsante **Applica**.

  ↬ Le impostazioni vengono registrate. La finestra di configurazione rimane aperta.

Se si desidera terminare la configurazione senza memorizzare le impostazioni:

- Fare clic sul pulsante **Annulla**.

  ↬ La finestra di configurazione si chiude e le impostazioni vengono ignorate.

Se si desidera ripristinare tutte le impostazioni dei valori standard nella configurazione:

- Fare clic su **Valori standard**.

↳ Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.

Opzioni di configurazione in sintesi

Esistono le seguenti opzioni di configurazione:

- **System Scanner**: Configurazione della scansione diretta
  - Opzioni di ricerca
  - Azioni in caso di rilevamento
  - Opzioni per la scansione degli archivi
  - Eccezioni della scansione diretta
  - Euristica della scansione diretta
  - Impostazione della funzione di report
- **Realtime Protection**: Configurazione della scansione in tempo reale
  - Opzioni di ricerca
  - Azioni in caso di rilevamento
  - Eccezioni della scansione in tempo reale
  - Euristica della scansione in tempo reale
  - Impostazione della funzione di report
- **Mail Protection**: configurazione del servizio Mail Protection
  - Opzioni di ricerca: attivazione del monitoraggio degli account POP3, account IMAP, email in uscita (SMTP)
  - Azioni in caso di malware
  - Euristica della scansione di Mail Protection
  - Funzione AntiBot: server SMTP consentiti, mittenti email consentiti
  - Eccezioni della scansione di Mail Protection
  - Configurazione della memoria temporanea, svuota la memoria temporanea
  - Configurazione della banca dati training AntiSpam, svuota la banca dati training
  - Configurazione di un piè di pagina nelle email inviate
  - Impostazione della funzione di report
- **Web Protection**: configurazione del servizio Web Protection
  - Opzioni di ricerca, attivazione e disattivazione di Web Protection
  - Azioni in caso di rilevamento
  - Accesso bloccato:Tipi di file e tipi di MIME indesiderati, Filtro Web per URL noti indesiderati (malware, phishing ecc.)
  - Eccezioni della scansione di Web Protection: URL, tipi di dati, tipi di MIME
  - Euristica di Web Protection
  - Funzione Protezione bambini: filtro basato sui ruoli e limitazione temporale dell'utilizzo di Internet basata sui ruoli

- Impostazione della funzione di report
- **FireWall**: configurazione del FireWall
  - Impostazione delle regole adattatore
  - Impostazione personalizzata delle regole di applicazione
  - Elenco produttori affidabili (eccezioni per l'accesso di rete delle applicazioni)
  - Impostazioni avanzate: timeout per le regole, limitazione per file host di Windows, blocco del FireWall di Windows, notifiche
  - Impostazioni pop up (avvisi per l'accesso di rete delle applicazioni)
- **Backup**:
  - Impostazione del componente Backup (backup incrementale, scansione di virus durante il backup)
  - Eccezioni: impostazione dei file da proteggere
  - Impostazione della funzione di report
- **Generale**:
  - Categorie estese delle minacce per la scansione diretta e in tempo reale
  - Protezione password per l'accesso al Control Center e alla configurazione
  - Sicurezza: indicatore di stato aggiornamento, indicatore di stato scansione completa del sistema, protezione del prodotto
  - WMI: attiva supporto WMI
  - Configurazione del log eventi
  - Configurazione delle funzioni di report
  - Impostazione delle directory utilizzate
  - Aggiornamento: configurazione del collegamento al server di download, impostazione dell'aggiornamento del prodotto
  - Configurazione degli avvisi acustici in caso di rilevamento malware

4.1.3 Icona Tray

Dopo l'installazione, l'icona Tray del prodotto Avira è collocata nella barra delle applicazioni:

Simbolo	Descrizione
	Realtime Protection di Avira e anche il FireWall sono attivati
	Realtime Protection di Avira è disattivato oppure il FireWall è disattivato

L'icona Tray mostra lo stato dei servizi Realtime Protection e FireWall.

Le funzioni principali del prodotto Avira sono facilmente accessibili mediante il menu contestuale dell'icona Tray.

- Per richiamare il menu contestuale, fare clic con il tasto destro del mouse sull'icona Tray.

Voci del menu contestuale

- **Attivazione di Realtime Protection**: attiva o disattiva il servizio Realtime Protection di Avira.
- **Attivazione di Mail Protection**: attiva o disattiva il servizio Mail Protection di Avira.
- **Attivazione di Web Protection**: attiva o disattiva il servizio Web Protection di Avira.
- **FireWall**:
  - Attiva FireWall: attiva o disattiva il FireWall
  - Blocca tutto il traffico: Attivata: blocca ogni trasferimento dati con l'eccezione dei trasferimenti al proprio sistema (Local Host / IP 127.0.0.1).
  - Attiva modalità di riproduzione: attiva o disattiva la modalità:
Attivata: vengono utilizzate tutte le regole di applicazione e le regole definite per l'adattatore. Viene consentito l'accesso alle applicazioni per le quali non è stata definita alcuna regola e non viene aperta nessuna finestra pop-up.
- **Avvio**: apre il Control Center.
- **Configurazione di Avira**: apre la Configurazione.
- **Avvia aggiornamento**: avvia un aggiornamento.
- **Guida in linea**: Apre la Guida in linea.
- **Informazioni su Avira Internet Security 2012:** apre una finestra di dialogo con informazioni sul prodotto Avira in uso: Informazioni su prodotto, versione e licenza.
- **Avira su Internet**: Apre il portale Web di Avira in Internet. Il prerequisito essenziale è l'accesso attivo a Internet.

4.2 Come procedere

4.2.1 Attiva licenza

In questo modo si attiva la licenza del prodotto Avira:

Con il file di licenza *hbedv.key* si attiva la licenza del prodotto Avira in uso. Il file di licenza viene inviato per email da Avira. Il file di licenza contiene la licenza per tutti i prodotti che si acquistano con un unico ordine.

Se il prodotto Avira non è ancora stato installato:

- salvare il file di licenza in una directory locale sul computer.
- Installare il prodotto Avira.

- Durante l'installazione indicare dove si è memorizzato il file di licenza.

Se il prodotto Avira è già stato installato:

- fare doppio clic sul file di licenza nel Filemanager o nell'email di attivazione e seguire le istruzioni delle schermate del sistema di gestione della licenza aperto.

  \- OPPURE -

  Nel Control Center del prodotto Avira in uso selezionare la voce di menu **Guida in linea > Gestione delle licenze**.

> **Suggerimenti**
> In Windows Vista appare la finestra di dialogo **Controllo Utente (User Account Control)**. Registrarsi come amministratore. Fare clic su **Prosegui**.

- Selezionare il file di licenza e fare clic su **Apri**.

  ↳ Apparirà un messaggio.

- Confermare con **OK**.

  ↳ La licenza è attivata.

- Riavviare il computer.

4.2.2 Rinnova licenza

È possibile rinnovare automaticamente la licenza del prodotto Avira in uso come descritto di seguito:

È possibile rinnovare automaticamente la licenza per il prodotto Avira in uso attivando l'opzione corrispondente nella sezione per il rinnovo delle licenze del negozio online.

Se il prodotto Avira non è ancora stato installato:

- Selezionare il prodotto desiderato nel negozio online di Avira.
- Selezionare l'opzione **Rinnovo automatico licenza alla scadenza**.
- Fare clic su **Avanti** per visualizzare i dati relativi al proprio ordine.
- Attivare anche qui l'opzione **Rinnovo automatico licenza alla scadenza**.
- Accettare le condizioni di licenza del software.
- Fare clic su **Completa l'ordine** per memorizzare il job e inoltrarlo ad Avira.

Se il prodotto Avira è già stato installato:

- Fare clic su **Stato** nella barra laterale di sinistra del Control Center.

  Fare clic su **Rinnova** accanto a *Prodotto attivato fino al...*

- La richiesta viene reindirizzata alla sezione *Panoramica delle licenze* dell'homepage di Avira.

↳ Nella sezione di panoramica delle licenze è possibile visualizzare i prodotti Avira per cui si dispone di licenza. In tale area è possibile modificare lo stato del prodotto e attivare o disattivare l'opzione **Rinnovo automatico licenza alla scadenza**. Questa opzione offre la possibilità di attivare o disattivare un rinnovo automatico della licenza. Nel caso in cui una licenza non sia idonea per l'estensione automatica della durata, viene visualizzato *Non disponibile*. Modificare lo stato facendo clic su **ON** o su **OFF**. Cambiando lo stato del rinnovo automatico della licenza da **ON** a **OFF**, viene visualizzato un messaggio di conferma ad indicare che la durata della licenza non può più essere estesa automaticamente.

- Fare clic su **OK** per confermare.

↳ Cambiando lo stato del rinnovo della licenza da **OFF** a **ON**, viene visualizzato un suggerimento ad indicare che la durata della licenza verrà estesa automaticamente 35 giorni prima della scadenza della licenza attualmente valida.

- Fare clic su **OK** per confermare il suggerimento.

↳ Se l'opzione **Rinnovo automatico licenza alla scadenza** è attivata, la data di scadenza della licenza viene visualizzata nella riga del prodotto.

- Specificare il proprio indirizzo email nel campo **Invio licenze a:...**, quindi fare clic su **Invia**.

↳ Se è stata selezionata l'opzione **Rinnovo automatico della licenza alla scadenza**, Avira ricorda all'utente l'imminente rinnovo automatico della licenza inviando un'email 40 giorni prima della scadenza della licenza stessa.

4.2.3 Attiva il prodotto

Per attivare il prodotto Avira in uso, sono disponibili le seguenti opzioni:

- Attivazione con una licenza completa valida

  Per attivare il programma con una licenza completa, è necessario disporre di una chiave di attivazione valida che comprende i dati della licenza acquistata. La chiave di attivazione è stata inviata per email oppure è indicata sulla confezione del prodotto.

- Attivazione con una licenza di evaluation

  Il prodotto Avira viene attivato tramite una licenza di evaluation generata automaticamente che consente all'utente di testare il prodotto Avira stesso e tutte le relative funzioni per un periodo di tempo limitato.

> **Suggerimenti**
> Per attivare il prodotto o richiedere una licenza di prova, è necessario disporre di una connessione Internet attiva.
> Nel caso non sia possibile stabilire una connessione ai server di Avira, controllare eventualmente le impostazioni del firewall utilizzato: durante

l'attivazione del prodotto vengono utilizzate connessioni tramite il protocollo HTTP e la porta 80 (comunicazione Web) e tramite il protocollo di codifica SSL e la porta 443. Assicurarsi che il proprio firewall non blocchi i dati in entrata o in uscita. Controllare inoltre che il proprio browser Web sia in grado di richiamare pagine Web.

Attivare il prodotto Avira nel modo seguente:

Se il prodotto Avira non è ancora stato installato:

- Installare il prodotto Avira.
  - ↳ Durante l'installazione viene richiesto all'utente di selezionare un'opzione di attivazione
- **Attiva il prodotto**= attivazione con una licenza completa valida
- **Prova il prodotto**= attivazione con una licenza di evaluation
- Per l'attivazione con una licenza completa, inserire la chiave di attivazione.
- Confermare la scelta della procedura di attivazione con **Avanti**.
- Inserire eventualmente i propri dati personali per la registrazione e confermare con **Avanti**.
  - ↳ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente. Il prodotto Avira è attivato.
- Continuare l'installazione.

Se il prodotto Avira è già stato installato:

- Nel Control Center selezionare la voce di menu **Guida in linea > Gestione delle licenze**.
  - ↳ Verrà avviato l'assistente per l'installazione della licenza, con cui è possibile selezionare un'opzione di attivazione. I passaggi successivi per l'attivazione del prodotto sono analoghi alla procedura descritta in precedenza.

4.2.4 Eseguire gli aggiornamenti automatici

Con la seguente procedura è possibile impostare con lo Scheduler Avira un job con cui aggiornare automaticamente il prodotto Avira:

- Selezionare in Control Center la rubrica **Gestione > Scheduler**.
- Fare clic sul simbolo + **Crea nuovo job con un wizard**.
  - ↳ Appare la finestra di dialogo **Nome e descrizione del job**.
- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.
  - ↳ Viene visualizzata la finestra di dialogo **Tipo di job**.

- Selezionare un **Job di aggiornamento** dalla lista.
- Fare clic su **Avanti**.
  - ↳ Apparirà la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguita la scansione:

- **Immediato**
- **Giornaliero**
- **Settimanale**
- **Intervallo**
- **Unico**
- **Login**

> **Suggerimenti**
> Raccomandiamo di eseguire gli aggiornamenti periodicamente e con una certa frequenza. L'intervallo di aggiornamento consigliato è: 2 Ore.

- Indicare il termine in base alla selezione.
- Selezionare una delle opzioni aggiuntive (disponibili in base al tipo di job):

- **Ripeti job se il tempo è già scaduto**
  Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
- **Avvia job quando si attiva connessione Internet (dial-up)**
  Oltre alla frequenza stabilita il job viene eseguito quando si attiva una connessione a Internet.

- Fare clic su **Avanti**.
  - ↳ Appare la finestra di dialogo **Selezione della modalità di visualizzazione**.
- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotta**: solo la barra di progressione
- **Estesa**: tutta la finestra del job

- Fare clic su **Fine**.
  - ↳ Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica **Gestione > Scansiona** come attivato (segno di spunta).
- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

i Visualizza le proprietà di un job

Modifica job

Elimina job

Avvia job

Arresta job

4.2.5 Avvio di un aggiornamento manuale

Sono disponibili varie opzioni per avviare manualmente un aggiornamento: durante gli aggiornamenti avviati manualmente viene sempre eseguito anche l'aggiornamento del file di definizione dei virus e del motore di ricerca. L'aggiornamento del prodotto avviene soltanto se nella configurazione in Sicurezza del computer > Aggiornamento > Aggiornamento prodotto è stata attivata l'opzione **Scarica aggiornamenti del prodotto e installa automaticamente**.

L'aggiornamento manuale del prodotto Avira può essere avviato nel modo seguente:

- Fare clic con il tasto destro del mouse sull'icona Tray di Avira nella barra delle applicazioni e selezionare **Avvia aggiornamento**.

  \- OPPURE -

- Nel Control Center selezionare la rubrica **Panoramica > Stato**, quindi fare clic nella sezione **Ultimo aggiornamento** sul link **Avvia aggiornamento**.

  \- OPPURE -

  In Control Center, nel menu **Aggiornamento** selezionare il comando **Avvia aggiornamento**.

  ↪ Compare la finestra di dialogo **Updater**.

> **Suggerimenti**
> Raccomandiamo di eseguire gli aggiornamenti automatici periodicamente. L'intervallo di aggiornamento consigliato è: 2 Ore.

> **Suggerimenti**
> É possibile eseguire un aggiornamento anche manualmente mediante il Centro di sicurezza Windows.

4.2.6 Scansione diretta: Eseguire il controllo di virus e malware con un profilo di ricerca

Un profilo di ricerca è un insieme di drive e directory che devono essere scansionati.

Per effettuare una scansione con un profilo di ricerca è possibile:

- Utilizzare il profilo di ricerca predefinito

  Se i profili di ricerca predefiniti si adattano alle proprie esigenze.

- Modificare il profilo di ricerca e utilizzarlo (selezione manuale)

  Se si desidera eseguire una scansione con un profilo di ricerca personalizzato.

- Creare e utilizzare un nuovo profilo

  Se si desidera salvare un profilo di ricerca personale.

In base al sistema operativo sono disponibili diversi simboli per l'avvio di un profilo di ricerca:

- In Windows XP e 2000:

   Con questo simbolo si avvia la scansione mediante un profilo di ricerca.

- In Windows Vista:

  In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

  Con questo simbolo si avvia una scansione limitata mediante un profilo di ricerca. Vengono scansionati solo i file e le directory per cui Windows Vista ha concesso i diritti di accesso.

  Con questo simbolo si avvia una scansione con diritti avanzati dell'amministratore. Dopo una conferma, vengono scansionati tutti i file e le directory del profilo di ricerca selezionato.

Per cercare virus e malware con un profilo:

- Selezionare la rubrica **Sicurezza del computer > System Scanner** nel Control Center.

  ↳ Appaiono i profili di ricerca predefiniti.

- Selezionare un profilo di ricerca predefinito.

  \- OPPURE -

  Modificare il profilo di ricerca **Selezione manuale**.

  \- OPPURE -

  Creare un nuovo profilo di ricerca

- Fare clic sul simbolo (Windows XP: o Windows Vista:).
- Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

Se si desidera modificare un profilo di ricerca:

- Aprire nel profilo di ricerca **Selezione manuale** la struttura dei file fin quando non vengono aperti tutti i drive e le directory che devono essere scansionati
- Fare clic sul segno **+**: viene visualizzato il livello della directory.
- Fare clic sul segno **-**: viene nascosto il livello della directory.
- Selezionare i nodi e le directory che devono essere scansionati facendo clic nella rispettiva casella dei vari livelli di directory

  Si hanno le seguenti possibilità per selezionare le directory:

- Directory incluse le sottodirectory (segno di spunta nero)
- Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
- Nessuna directory (nessun segno di spunta)

Se si desidera creare un nuovo profilo di ricerca:

- Fare clic sul simbolo **Crea nuovo profilo.**
  - ↳ Il *Nuovo profilo* appare sotto quelli già esistenti.
- Assegnare un nome al profilo di ricerca facendo clic sul simbolo .
- Evidenziare altri punti e directory che devono essere verificati con un clic nella casella del livello della directory.

  Si hanno le seguenti possibilità per selezionare le directory:

- Directory incluse le sottodirectory (segno di spunta nero)
- Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
- Nessuna directory (nessun segno di spunta)

4.2.7 Scansione diretta: Ricerca di virus e malware con Drag & Drop

È possibile cercare con Drag&Drop virus e malware nel modo seguente:

- ✓ Il Control Center del programma Avira è aperto.
- Selezionare il file o la directory, che si desidera controllare.
- Trascinare con il tasto sinistro del mouse il file selezionato o la directory selezionata nel Control Center.
  - ↳ Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.

↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.2.8 Scansione diretta: Cerca virus e malware con il menu contestuale

Per cercare in maniera mirata virus e malware mediante il menu contestuale:

- Fare clic (ad esempio in Esplora risorse di Windows, sul desktop o in una directory aperta di Windows) con il tasto destro del mouse sul file o sulla directory che si desidera controllare.
  - ↳ Appare il menu contestuale di Esplora risorse di Windows.
- Nel menu contestuale selezionare **Controlla i file selezionati con Avira**.
  - ↳ Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.2.9 Scansione diretta: cerca automaticamente virus e malware

> **Suggerimenti**
> Una volta eseguita l'installazione il job *Scansione completa del sistema* si trova nello : in un intervallo di aggiornamento consigliato viene eseguita automaticamente una scansione completa del sistema.

Cercare automaticamente virus e malware è un job che si imposta come segue:

- Selezionare in Control Center la rubrica **Gestione > Scheduler**.
- Fare clic sul simbolo + **Crea nuovo job con un wizard**.
  - ↳ Appare la finestra di dialogo **Nome e descrizione del job**.
- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.
  - ↳ Appare la finestra di dialogo **Tipo di job**.
- Selezionare il **Job di scansione**.
- Fare clic su **Avanti**.
  - ↳ Appare la finestra di dialogo **Selezione del profilo**.
- Selezionare quale profilo deve essere scansionato.
- Fare clic su **Avanti**.
  - ↳ Apparirà la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguita la scansione:

▪ **Immediato**
▪ **Giornaliero**

- **Settimanale**
- **Intervallo**
- **Unico**
- **Login**

- Indicare il termine in base alla selezione.
- Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job): **Ripeti job se il tempo è già scaduto**

  ↳ Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

- Fare clic su **Avanti**.

  ↳ Appare la finestra di dialogo **Selezione della modalità di visualizzazione**.

- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotta**: solo la barra di progressione
- **Estesa**: tutta la finestra del job

- Selezionare l'opzione **Spegni computer al termine del job**, se si desidera che il calcolatore si spenga automaticamente non appena il job è stato eseguito e concluso.

  L'opzione è disponibile solo nella modalità di visualizzazione ridotta o estesa.

- Fare clic su **Fine**.

  ↳ Il nuovo job assegnato viene visualizzato nella pagina iniziale della rubrica **Gestione > Scheduler** come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

4.2.10 Scansione diretta: Effettuare una scansione mirata per rootkit attivi

Per effettuare una ricerca di rootkit attivi, utilizzare il profilo di ricerca predefinito **Cerca rootkit e malware attivi**.

La ricerca di rootkit mirata si effettua nel modo seguente:

- Selezionare la rubrica **Sicurezza del computer > System Scanner** nel Control Center.
  - ↳ Appaiono i profili di ricerca predefiniti.
- Selezionare il profilo di ricerca predefinito **Cerca rootkit e malware attivi**.
- Evidenziare altri punti e directory che devono essere verificati con un clic nella casella del livello della directory.
- Fare clic sul simbolo (Windows XP: o Windows Vista:).
  - ↳ Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.2.11 Reagire a virus e malware riscontrati

Per i singoli componenti di protezione del prodotto Avira in uso, è possibile impostare nella configurazione, nella rubrica **Azione in caso di rilevamento**, il modo in cui tale prodotto deve reagire al rilevamento di un virus o di un programma indesiderato.

Nel componente ProActiv di Realtime Protection non esiste la possibilità di configurare alcuna opzione di azione: un rilevamento viene sempre comunicato nella finestra **Realtime Protection: Comportamento sospetto di un'applicazione**.

Opzioni di azione in System Scanner:

- **Interattivo**

  Nella modalità di azione interattiva vengono notificati i rilevamenti della scansione di System Scanner in una finestra di dialogo. Questa opzione è attivata di default.
  Al termine della scansione di System Scanner, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione di System Scanner.
- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Realtime Protection:

- **Interattivo**

Nella modalità di azione interattiva viene negato l'acceso ai dati e sul desktop viene visualizzato un messaggio. È possibile rimuovere il malware rilevato direttamente nel messaggio sul desktop oppure trasmetterlo al componente System Scanner per un ulteriore trattamento del virus selezionando il pulsante **Dettagli**. System Scanner segnala il rilevamento in una finestra, nella quale, mediante un menu contestuale, sono disponibili diverse opzioni per il trattamento del file infetto (vedere Rilevamento > System Scanner).

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Mail Protection, Web Protection:

- **Interattivo**

  Nella modalità di azione interattiva, in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come gestire i file infetti. Questa opzione è attivata di default.

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Modalità di azione interattiva

- Nella modalità di azione interattiva si reagisce ai virus e ai programmi indesiderati rilevati selezionando nell'avviso un'azione per gli oggetti infetti ed eseguendo l'azione selezionata mediante conferma.

Per il trattamento di oggetti infetti possono essere selezionate le seguenti azioni:

> **Suggerimenti**
> Le azioni disponibili dipendono dal sistema operativo, dal componente di protezione (Avira System Scanner, Avira Realtime Protection, Avira Mail Protection, Avira Web Protection) che segnala il file rilevato e dal malware rilevato.

Azioni di System Scanner e di Realtime Protection (senza rilevamenti di ProActiv):

- **Ripara**

  Il file viene riparato.
  Questa opzione è attivabile solo se è possibile riparare il file.

- **Rinomina**

Il file viene rinominato **.vir*. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

- **Quarantena**

  Il file viene compresso in un formato speciale (**.qua*) e spostato nella directory di quarantena *INFECTED* sull'hard disk, in modo da escludere qualsiasi accesso diretto. I file in questa directory possono essere successivamente riparati nella quarantena o, se necessario, inviati ad Avira.

- **Elimina**

  Il file viene eliminato.Questa procedura è più rapida di **Sovrascrivi ed elimina**. Se il file rilevato è un virus del record di avvio eliminarlo con Elimina. Viene scritto un nuovo record di avvio.

- **Ignora**

  Non viene eseguita alcuna altra azione. Il file infetto rimane attivo sul computer.

- **Sovrascrivi ed elimina**

  Il file viene sovrascritto con un modello e, infine, eliminato. Il file non può essere ripristinato.

> **Attenzione**
> Pericolo di perdita di dati e danni al sistema operativo!
> Utilizzare l'opzione **Ignora** solo in casi eccezionali e fondati.

- **Ignora sempre**

  Opzione di azione in caso di file rilevati da Realtime Protection: Realtime Protection non esegue alcuna altra azione. L'accesso al file viene autorizzato. Vengono autorizzati tutti gli accessi successivi a questo file e non si ricevono comunicazioni fino al riavvio del computer o a un aggiornamento del file di definizione dei virus.

- **Copia in quarantena**

  Opzione di azione in caso di rilevamento di un Rootkits: il file rilevato viene copiato nella quarantena.

- **Ripara record di avvio | Scarica strumento di riparazione**

  Opzioni di azione in caso di rilevamento di record di avvio infetto: in caso di drive del floppy disk infetti sono disponibili opzioni per effettuare la riparazione. Se con il prodotto Avira non è possibile effettuare alcuna riparazione, è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

> **Suggerimenti**
> Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

Azioni di Realtime Protection in caso di file rilevati dal componente ProActiv (messaggio di azioni sospette di un'applicazione):

- **Programma attendibile**

  L'esecuzione dell'applicazione prosegue. Il programma viene inserito nell'elenco delle applicazioni consentite ed escluso dal monitoraggio mediante il componente ProActiv. Aggiungendolo nell'elenco delle applicazioni consentite viene impostato il tipo di monitoraggio *Contenuti*. Questo significa che l'applicazione viene esclusa dal monitoraggio mediante il componente ProActiv solo in caso di contenuti non modificati (vedere Filtro delle applicazioni: Applicazioni da escludere).

- **Blocca il programma una volta**

  L'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene terminata. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

- **Blocca sempre questo programma**

  L'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene terminata. Il programma viene inserito nell'elenco delle applicazioni da bloccare e non può più essere eseguito (vedere Filtro delle applicazioni: Applicazioni da bloccare).

- **Ignora**

  L'esecuzione dell'applicazione prosegue. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

Azioni di Mail Protection: Email in ingresso

- **Sposta in quarantena**

  L'email viene spostata in Quarantena unitamente agli allegati. L'email infetta viene eliminata. Il corpo del testo e gli allegati delle email vengono sostituiti da un testo standard.

- **Elimina email**

  L'email infetta viene eliminata. Il corpo del testo e gli allegati delle email vengono sostituiti da un testo standard.

- **Elimina allegato**

  L'allegato infetto viene sostituito da un testo standard. Se il corpo del testo dell'email risulta infetto, viene eliminato ed eventualmente sostituito da un testo standard. L'email stessa viene inoltrata.

- **Sposta allegato in quarantena**

  L'allegato infetto viene collocato in Quarantena e infine eliminato (sostituito da un testo standard). Il corpo dell'email viene inoltrato. L'allegato infetto potrà essere successivamente inoltrato con il Gestore della quarantena.

- **Ignora**

  L'email infetta viene inoltrata.

> **Attenzione**
> In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali. Disattivare l'anteprima in Microsoft Outlook, non aprire mai gli allegati facendo doppio clic!

Azioni di Mail Protection: Email in uscita

- **Sposta email in quarantena (non inviare)**

  L'email unitamente agli allegati viene copiata in Quarantena e non inviata. L'email resta nella Posta in uscita del client email. Nel programma email viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

- **Blocca invio email (non inviare)**

  L'email non viene inviata e resta nella Posta in uscita del client email. Nel programma email viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

- **Ignora**

  Le email infette vengono inviate.

> **Attenzione**
> In questo modo virus e programmi indesiderati potrebbero raggiungere il computer del destinatario dell'email.

Azioni di Web Protection:

- **Nega accesso**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso.

- **Quarantena**

  Il sito web richiesto dal server web o i dati e i file trasferiti non vengono spostati nella quarantena. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

- **Ignora**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web.

Attenzione
In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali.

Suggerimenti
Consigliamo di spostare in quarantena un file sospetto che non può essere riparato.

Suggerimenti
Inviare a noi i file da analizzare che sono stati segnalati dall'euristica.
É possibile caricare i file ad esempio dal nostro sito web:
http://www.avira.it/sample-upload
I file segnalati dall'euristica si riconoscono dalla definizione *HEUR/* o *HEURISTIC/*, che viene anteposta al nome del file, ad esempio: *HEUR/provafile.**.

4.2.12 Quarantena: Trattare file (*.qua) in quarantena

É possibile trattare i file in quarantena nel modo seguente:

- Selezionare la rubrica **Gestione > Quarantena** nel Control Center.
- Verificare di quali file si tratta cosicché sia possibile ripristinare gli originali sul computer.

Se si desidera visualizzare maggiori informazioni su un file:

- Selezionare il file e fare clic su [i].
  - ↳ Apparirà la finestra di dialogo **Proprietà** con ulteriori informazioni sul file.

Se si desidera verificare nuovamente un file:

La verifica di un file è consigliata quando il file di definizione dei virus del prodotto Avira è stato aggiornato ed esiste il sospetto di un falso allarme. É così possibile confermare un falso allarme a una successiva verifica e ripristinare il file.

- Selezionare il file e fare clic su [lente].
  - ↳ Il file viene controllato utilizzando le impostazioni della scansione diretta per virus e malware.
  - ↳ Dopo il controllo appare la finestra di dialogo **Statistiche della scansione** che visualizza la statistica relativa allo stato del file prima e dopo la nuova scansione.

Se si desidera eliminare un file:

- Selezionare il file e fare clic su .
- Occorre confermare la selezione effettuata mediante **Sì**.

Se si desidera caricare il file da analizzare su un server Web di Avira Malware Research Center:

- Selezionare il file che si desidera caricare.
- Fare clic su .
  - ↪ Si aprirà la finestra di dialogo *Carica file* con un modulo per inserire i dati personali a cui essere contattati.
- Indicare per intero i propri dati.
- Selezionare un tipo: **File sospetto** oppure **Sospetto di Falso allarme**.
- Selezionare un formato di risposta: **HTML**, **Testo**, **HTML & Testo**.
- Fare clic su **OK**.
  - ↪ Il file compresso viene caricato su un server Web di Avira Malware Research Center.

Suggerimenti
Nei seguenti casi si consiglia un'analisi da parte di Avira Malware Research Center:
Oggetto euristico (file sospetto): durante una scansione, un file del prodotto Avira è stato identificato come sospetto e spostato in quarantena: Nella finestra di dialogo per il rilevamento di virus o nel file di report della scansione è stata consigliata l'analisi del file da parte di Avira Malware Research Center.
File sospetto: Il file ritenuto sospetto è stato aggiunto alla quarantena, tuttavia la verifica del file per virus e malware ha dato esito negativo.
Sospetto di Falso allarme: Si parte dal presupposto che si tratti di un falso allarme nel rilevamento di un virus: Il prodotto Avira indica un rilevamento in un file che tuttavia con tutta probabilità non è infetto da malware.

Suggerimenti
La dimensione dei file caricati si limita a 20 MB non compressi o a 8 MB compressi.

Suggerimenti
È possibile caricare solo un singolo file.

Se si desidera copiare un oggetto in quarantena in un altra directory:

- Selezionare il file in quarantena e fare clic su .

  ↳ Si apre la finestra *Cerca cartella* in cui è possibile selezionare una directory.
- Selezionare una directory nella quale deve essere archiviata una copia dell'oggetto in quarantena e confermare con **OK**.
  ↳ L'oggetto in quarantena selezionato viene archiviato nella directory scelta.

Suggerimenti
L'oggetto in quarantena non è uguale al file ripristinato. L'oggetto in quarantena è crittografato e non può essere eseguito o letto nel formato originale.

Se si desidera esportare in un file di testo le proprietà di un oggetto in quarantena selezionato:

- Selezionare il file in quarantena e fare clic su .
  ↳ Si apre il file di testo *Quarantena - Editor* con i dati dell'oggetto in quarantena scelto.
- Salvare il file di testo.

I file in quarantena possono anche essere ripristinati (vedere Capitolo: Quarantena: Ripristina file in quarantena

4.2.13 Quarantena: Ripristina file in quarantena

In base al sistema operativo sono disponibili diversi sistemi per il ripristino:

- **In Windows XP e 2000**:

  Con questo simbolo si ripristinano i file nella directory originale.

  Con questo simbolo si ripristinano i file nella directory selezionata.
- **In Windows Vista**:

  In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

  Con questo simbolo si ripristinano i file nella directory selezionata.

  Con questo simbolo si ripristinano i file nella directory originale. Se per l'accesso a questa directory sono necessari diritti di amministratore avanzati, appare una richiesta corrispondente.

É possibile ripristinare i file in quarantena nel modo seguente:

Attenzione
Pericolo di perdita di dati e danni al sistema operativo del computer! Utilizzare la funzione **Ripristina l'oggetto selezionato** solo in casi eccezionali. Ripristinare solo quei file che possono essere riparati con una nuova scansione.

✓ File nuovamente controllato e riparato con una scansione.

- Selezionare la rubrica **Gestione > Quarantena** nel Control Center.

Suggerimenti

Le email e gli allegati possono essere ripristinati solo con l'opzione e con l'estensione **.eml*.

Se si desidera ripristinare un file nella sua posizione originale:

- Evidenziare il file e fare clic sul simbolo (Windows 2000/XP: , Windows Vista).

Questa opzione non è disponibile per le email.

Suggerimenti

Le email e gli allegati possono essere ripristinati solo con l'opzione e con l'estensione **.eml*.

↳ Viene richiesto quindi se si desidera ripristinare il file.

- Fare clic su **Sì**.

↳ Il file viene ripristinato nella directory dalla quale è stato spostato in quarantena.

Se si desidera ripristinare un file in una determinata directory:

- Selezionare il file e fare clic su .

↳ Viene richiesto quindi se si desidera ripristinare il file.

- Fare clic su **Sì**.

↳ Apparirà la finestra standard di Windows per la selezione di una directory.

- Selezionare la directory nella quale si desidera ripristinare il file e confermare.

↳ Il file viene ripristinato nella directory selezionata.

4.2.14 Quarantena: Sposta i file sospetti in quarantena

É possibile spostare in quarantena i file sospetti manualmente come segue:

- Selezionare la rubrica **Gestione > Quarantena** nel Control Center.
- Fare clic su [+].
  - ↳ Apparirà la finestra standard di Windows per la selezione di un file.
- Selezionare il file e confermare con **Apri**.
  - ↳ Il file viene spostato in quarantena.

È possibile controllare i file in quarantena con Avira System Scanner (vedere Capitolo: Quarantena: Trattare file (*.qua) in quarantena).

4.2.15 Profilo di ricerca: Inserisci o elimina un tipo di file in un profilo di ricerca

Per stabilire per un profilo di ricerca i tipi di file da scansionare o i tipi di file che devono essere esclusi dalla ricerca (possibile solo con selezione manuale e profili di ricerca personalizzati):

✓ In Control Center, nella rubrica **Sicurezza del computer > Verifica**.

- fare clic con il tasto destro del mouse sul profilo di ricerca che si desidera modificare.
  - ↳ Apparirà un menu contestuale.
- Selezionare la voce **Filtro file**.
- Aprire nuovamente il menu contestuale facendo clic sul piccolo triangolo sul lato destro del menu contestuale.
  - ↳ Appariranno le voci **Standard**, **Controlla tutti i file** e **Personalizzato**.
- Selezionare la voce **Personalizzato**.
  - ↳ Apparirà la finestra di dialogo **Estensione file** con un elenco di tutti i tipi di file che devono essere abbinati al profilo di ricerca.

Se si desidera escludere un tipo di file dalla scansione:

- Selezionare il tipo di file e fare clic su **Elimina**.

Se si desidera aggiungere un tipo di file dalla scansione:

- Selezionare un tipo di file.
- Fare clic su **Aggiungi** e inserire l'estensione del tipo di file nel campo.

  Utilizzare un massimo di 10 caratteri e non inserire punti. Le wildcard (* e ?) sono consentite.

4.2.16 Profilo di ricerca: Creare un collegamento sul desktop per il profilo di ricerca

Mediante un collegamento sul desktop per un profilo di ricerca è possibile avviare una scansione diretta facendo clic sul desktop senza richiamare il Control Center del prodotto Avira.

É possibile creare un collegamento al profilo di ricerca dal desktop:

✓ In Control Center, nella rubrica **Sicurezza del computer > Verifica**.

- selezionare il profilo di ricerca di cui si intende creare il collegamento.
- Fare clic sul simbolo .
  ↳ Viene creato un collegamento sul desktop.

4.2.17 Eventi: Filtrare eventi

Nel Control Center, in **Gestione > Eventi**, vengono visualizzati eventi creati dai componenti del prodotto Avira (analogamente al visualizzatore eventi del sistema operativo di Windows). Di seguito sono riportati i componenti del programma:

- Backup
- Web Protection
- Realtime Protection
- Mail Protection
- FireWall
- Servizio di assistenza
- Scheduler
- System Scanner
- Updater

Vengono visualizzati i seguenti tipi di eventi:

- *Informazioni*
- *Attenzione*
- *Errore*
- *Rilevamento*

Come filtrare gli eventi visualizzati:

- Selezionare nel Control Center la rubrica **Gestione > Eventi**.
- Attivare la casella delle componenti di programma per visualizzare gli eventi delle componenti attive.

- OPPURE -

Disattivare la casella di spunta dei componenti di programma per non visualizzare gli eventi dei componenti disattivati.

- Attivare la casella dei tipi di evento per visualizzare questi eventi.

  - OPPURE -

  Disattivare la casella di spunta dei tipi di evento per non visualizzare questi eventi.

4.2.18 Mail Protection: Escludere indirizzi email dalla scansione

È possibile impostare come segue gli indirizzi email (mittente) che devono essere esclusi dal controllo di Mail Protection (cosiddetta white list):

- Selezionare la rubrica **Sicurezza Internet > Mail Protection** nel Control Center.

  ↳ Nell'elenco vengono visualizzate le email in ingresso.

- Selezionare l'email che si desidera escludere dal controllo di Mail Protection.

- Fare clic sul simbolo desiderato per escludere l'email dal controllo di Mail Protection:

  L'indirizzo email selezionato non verrà più verificato per virus e programmi indesiderati.

  L'indirizzo email selezionato non verrà più verificato per lo spam.

  ↳ L'indirizzo email del mittente verrà inserito nell'elenco delle eccezioni e non verrà più verificato per virus, malwareo spam.

Attenzione
Escludere solo indirizzi email di mittenti assolutamente affidabili dal controllo di Mail Protection.

Suggerimenti
Nella configurazione in Mail Protection > Generale > Eccezioni è possibile inserire altri indirizzi email o eliminarne alcuni nell'elenco delle eccezioni.

4.2.19 Mail Protection: Configurare il modulo AntiSpam

Il modulo AntiSpam contiene una banca dati di configurazione. In questa banca dati vengono inseriti i criteri di categorizzazione definiti dall'utente. Nel corso del tempo si impostano quindi i filtri interni, gli algoritmi e i criteri di valutazione per lo spam in base ai propri criteri personali.

É possibile categorizzare le email per la banca dati come segue:

- Selezionare la rubrica **Sicurezza Internet > Mail Protection** nel Control Center.

↳ Nell'elenco è possibile vedere le email in entrata.

- Selezionare le email che si desidera categorizzare.
- Fare clic sul simbolo desiderato per contrassegnare l'email, ad esempio come *Spam* o come desiderata, ovvero come email "buona" .

↳ L'email viene inserita nella banca dati training e verrà utilizzata la volta successiva per il riconoscimento di spam.

> **Suggerimenti**
> È possibile eliminare la banca dati training nella configurazione tramite **Mail Protection > Generale > AntiSpam**.

4.2.20 FireWall: Selezionare il livello di sicurezza per il FireWall

É possibile scegliere tra diversi livelli di sicurezza. In base ad esse si ha la possibilità di scegliere diverse possibilità di configurazione per le regole adattatore.

Sono disponibili i seguenti livelli di sicurezza:

- **Basso**

  Il flooding e il Port-Scan vengono riconosciuti.

- **Medio**

  I pacchetti TCP e UDP sospetti vengono respinti.
  Vengono impediti il flooding e il Port-Scan.
  (impostazione standard)

- **Elevato**

  Il computer non è visibile sulla rete.
  I collegamenti dall'esterno vengono bloccati.
  Vengono impediti il flooding e il Port-Scan.

- **Utente**

  Regole personalizzate: con questo livello di sicurezza il programma è automaticamente convertito se sono state modificate le regole adattatore.

> **Suggerimenti**
> L'impostazione standard del livello di sicurezza per tutte le regole predefinite di Avira FireWall è **Medio**.

É possibile impostare il livello di sicurezza del FireWall come segue:

- Selezionare la rubrica **Sicurezza Internet > FireWall** nel Control Center.
- Impostare il cursore di riempimento sul livello di sicurezza desiderato.

↳ Il livello di sicurezza scelto è attivo subito dopo la selezione.

4.2.21 Backup: Creazione manuale di backup

Lo strumento Backup nel Control Center consente di creare in modo semplice e rapido un backup dei dati personali.Backup di Avira consente di creare i cosiddetti backup speculari, con i quali è possibile eseguire il backup dei dati e mettere a disposizione i dati più aggiornati risparmiando risorse. Durante la memorizzazione con Backup di Avira è possibile verificare i dati da mettere al sicuro da virus e malware. I file infetti non vengono salvati.

> **Suggerimenti**
> Nei backup speculari, a differenza di quelli delle versioni, non vengono mantenute singole versioni del backup. Il backup speculare contiene lo stato dei dati al momento dell'ultimo backup. Se nel gruppo dei dati da sottoporre a backup vengono eliminati dei file, non avviene alcun confronto in occasione del backup successivo, ovvero i file eliminati sono ancora presenti nel backup.

> **Suggerimenti**
> Per impostazione predefinita Il Backup di Avira effettua il backup dei soli dati modificati ed effettua un controllo sulla presenza di virus e malware. Queste impostazioni si possono modificare nella configurazione in Backup > Impostazioni.

Per memorizzare i dati con lo strumento backup:

- Selezionare la rubrica **Sicurezza del computer > Backup** nel Control Center.

  ↳ Vengono visualizzati i profili di backup predefiniti.

- Selezionare un profilo di backup predefinito.

  \- OPPURE -

  Adeguare il profilo **Selezione manuale**.

  \- OPPURE -

  Creare un nuovo profilo di backup

- Nel campo **Directory di destinazione** immettere una destinazione di memorizzazione per il profilo selezionato.

  Come destinazione di memorizzazione per il backup è possibile selezionare una directory sul computer o su un drive di rete collegato nonché un supporto dati rimovibile, come una penna USB o un floppy disk.

- Fare clic sul simbolo .

↳ Viene visualizzata la finestra **Backup di Avira** e il backup si avvia. Lo stato e gli eventi del backup vengono visualizzati nella finestra di backup.

Se si desidera adeguare un profilo di backup:

- Aprire in **Selezione manuale** la struttura dei file fin quando non vengono aperti tutti i drive e le directory che devono essere memorizzati:

- Fare clic sul segno **+**: viene visualizzato il livello della directory.
- Fare clic sul segno **-**: viene nascosto il livello della directory.

- Selezionare i nodi e le directory da memorizzare facendo clic sulla casella di controllo corrispondente al singolo livello di directory:

  Si hanno le seguenti possibilità per selezionare le directory:

- Directory incluse le sottodirectory (segno di spunta nero)
- Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
- Nessuna directory (nessun segno di spunta)

Se si desidera creare un nuovo profilo di backup:

- Fare clic sul simbolo + **Crea nuovo profilo**.

  ↳ Il *Nuovo profilo* appare sotto quelli già esistenti.

- Rinominare eventualmente il profilo di backup facendo clic sul simbolo .
- Selezionare i nodi e le directory da memorizzare facendo clic sulla casella di controllo in ciascun livello directory.

  Si hanno le seguenti possibilità per selezionare le directory:

- Directory incluse le sottodirectory (segno di spunta nero)
- Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
- Nessuna directory (nessun segno di spunta)

4.2.22 Backup: Creazione di backup automatizzati

In questo modo si definisce un job che consente di creare backup automatizzati:

- Selezionare in Control Center la rubrica **Gestione > Scheduler**.
- Fare clic sul simbolo +.

  ↳ Appare la finestra di dialogo **Nome e descrizione del job**.

- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.

  ↳ Appare la finestra di dialogo **Tipo di job**.

- Selezionare **Job di backup**.
- Fare clic su **Avanti**.
  ↪ Appare la finestra di dialogo **Selezione del profilo**.
- Selezionare quale profilo deve essere scansionato.

Suggerimenti
Viene visualizzato esclusivamente il profilo di backup per il quale è stata immessa una destinazione di memorizzazione.

- Fare clic su **Avanti**.
  ↪ Apparirà la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguita la scansione:

- **Immediato**
- **Giornaliero**
- **Settimanale**
- **Intervallo**
- **Unico**
- **Login**
- **Plug&Play**

Per l'evento **Plug&Play** viene sempre creato un backup quando il supporto dati rimovibile selezionato come destinazione di memorizzazione per il profilo di backup viene collegato al computer. Per questo evento **Plug&Play**, è necessario avere definito una penna USB come destinazione di memorizzazione.

- Indicare il termine in base alla selezione.
- Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job): **Ripeti job se il tempo è già scaduto**
  ↪ Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
- Fare clic su **Avanti**.
  ↪ Appare la finestra di dialogo **Selezione della modalità di visualizzazione**.
- Selezionare la modalità di visualizzazione della finestra del job:

- **Ridotta**: solo la barra di progressione
- **Estesa**: l'intera finestra di backup
- **Invisibile**: nessuna finestra di backup

- Fare clic su **Fine**.
  ↪ Il nuovo job assegnato viene visualizzato nella pagina iniziale della rubrica **Gestione > Scheduler** come attivato (segno di spunta).
- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

Visualizza proprietà di un job

Modifica job

Elimina job

Avvia job

Arresta job

5. System Scanner

Con il componente System Scanner è possibile effettuare scansioni mirate per virus e programmi indesiderati (scansione diretta). È possibile effettuare una scansione per file infetti in diversi modi:

- **Scansione diretta mediante menu contestuale**
  La scansione diretta mediante il menu contestuale (tasto destro del mouse - voce **Controlla i file selezionati con Avira**) si consiglia quando, ad esempio, si desidera controllare singoli file e directory in Esplora risorse di Windows. Un ulteriore vantaggio è che il Control Center non deve essere avviato per la scansione diretta mediante il menu contestuale.
- **Scansione diretta con Drag & Drop**
  Trascinando un file o una directory nella finestra di programma del Control Center System Scanner verifica il file o la directory, nonché tutte le sottodirectory. Questa procedura è consigliata quando si desidera controllare i singoli file e directory che sono stati archiviati, ad esempio, sul desktop.
- **Scansione diretta per profili**
  Questa procedura è consigliata quando si desidera controllare regolarmente alcune directory e drive (ad esempio la propria directory di lavoro o drive, sui quali si archiviano regolarmente nuovi file). Queste directory e drive non devono quindi essere selezionati a ogni scansione ma vengono comodamente selezionati tramite il profilo corrispondente. Vedere Scansione diretta per profili.
- **Scansione diretta con Scheduler**
  offre la possibilità di far eseguire job temporizzati di scansione. Vedere Scansione diretta con Scheduler.

Durante la scansione per rootkit, virus del record di avvio e durante la scansione dei processi attivi sono necessari dei procedimenti particolari. Sono disponibili le seguenti opzioni:

- Cerca rootkit mediante il profilo di ricerca *Cerca rootkit e malware attivi*
- Scansione dei processi attivi mediante il profilo di ricerca *Processi attivi*
- Scansiona virus del record di avvio con il comando **Scansiona virus del record di avvio...** nel menu **Extra**

6. Aggiornamenti

L'efficacia di un software antivirus dipende dall'aggiornamento del programma, in particolare del file di definizione dei virus e del motore di ricerca. Per l'esecuzione degli aggiornamenti, il componente Updater è integrato nel prodotto Avira. Updater garantisce che il prodotto Avira sia sempre il più aggiornato possibile e che sia in grado di rilevare i nuovi virus che compaiono quotidianamente. Updater aggiorna i seguenti componenti:

- File di definizione dei virus:

  Il file di definizione dei virus contiene il modello di rilevamento del programma dannoso che il prodotto Avira utilizza nella scansione per virus e malware nonché nella riparazione di oggetti infetti.

- Motore di ricerca:

  Il motore di ricerca contiene i metodi che vengono utilizzati dal prodotto Avira per la scansione per virus e malware.

- File di programma (aggiornamento del prodotto):

  I pacchetti di aggiornamento del prodotto mettono a disposizione ulteriori funzioni per i singoli componenti del programma.

Durante un aggiornamento viene verificato lo stato di aggiornamento del file di definizione dei virus e del motore di ricerca e, se necessario, tali componenti vengono aggiornati. In base alle impostazioni di configurazione Updater esegue un aggiornamento del prodotto o segnala la disponibilità di tale aggiornamento. Terminato un aggiornamento del prodotto può essere necessario riavviare il sistema. Se l'aggiornamento avviene solo per il file di definizione dei virus e del motore di ricerca non è necessario riavviare il computer.

> **Suggerimenti**
> Per motivi di sicurezza, l'Updater verifica se il file host di Windows del computer è stato modificato, ad esempio con manipolazione da parte di malware dell'URL di aggiornamento, a seguito della quale l'Updater viene indirizzato su pagine di download indesiderate. Se il file host di Windows è stato manipolato, l'evento viene riportato nel file di report di Updater.

Un aggiornamento viene eseguito in automatico nel seguente intervallo: 2 Ore. È possibile modificare o disattivare l'aggiornamento automatico dalla configurazione (Configurazione > Aggiorna).

Nel Control Center sotto **Scheduler** è possibile configurare ulteriori job di aggiornamento che Updater deve eseguire a intervalli definiti. È inoltre possibile avviare l'aggiornamento manualmente:

- In Control Center: nel menu **Aggiornamento** e nella rubrica **Stato**
- Tramite il menu contestuale dell'icona Tray

Gli aggiornamenti vengono richiamati da Internet tramite un server Web del produttore. Normalmente si utilizza la connessione di rete esistente per collegarsi al server di download di Avira. Questa impostazione standard può essere modificata nella configurazione in Generale > Aggiorna.

7. FireWall

Avira FireWall monitora e regola il traffico dati in entrata e in uscita sul computer e lo protegge dai numerosi attacchi e minacce provenienti da Internet: in base alle direttive di sicurezza, il traffico dati in entrata e in uscita o l'attesa delle porte vengono consentiti o rifiutati. Quando Avira FireWall rifiuta le attività di rete bloccando così le connessioni Internet, si riceve un messaggio sul desktop. Sono disponibili le seguenti possibilità di impostazione di Avira FireWall:

mediante l'impostazione di un livello di sicurezza nel Control Center

In Control Center è possibile impostare un livello di sicurezza. I livelli di sicurezza *Basso*, *Medio* e *Alto* contengono ognuno più regole di sicurezza integrative basate su filtri di pacchetto. Queste regole di sicurezza vengono memorizzate come regole adattatore predefinite in FireWall > Regole adattatore.

memorizzando le azioni nella finestra Evento di rete

Se un'applicazione tenta per la prima volta di creare una connessione alla rete o a Internet, si apre la finestra pop up *Evento di rete*. Nella finestra *Evento di rete*, l'utente può scegliere se l'attività di rete dell'applicazione viene consentita o rifiutata. Se l'opzione **Memorizza azione per questa applicazione** è attivata, l'azione viene creata come regola di applicazione e memorizzata nella configurazione sotto **FireWall > Regole di applicazione**. Memorizzando le azioni nella finestra Evento di rete, si ottiene un set di regole per le attività di rete delle applicazioni.

Suggerimenti
In caso di applicazioni di fornitori affidabili, l'accesso alla rete viene consentito per default purché una regola adattatore non vieti l'accesso alla rete. È possibile rimuovere fornitori dall'elenco dei fornitori affidabili.

mediante la creazione di regole adattatore e di applicazione in Configurazione

Nella configurazione è possibile modificare le regole adattatore predefinite o crearne di nuove. Se si aggiungono o modificano le regole adattatore il livello di sicurezza del FireWall viene impostato automaticamente sul valore *Utente*.
Con le regole adattatore è possibile definire regole di monitoraggio specifiche per le applicazioni:
Con semplici regole di applicazione, è possibile impostare se tutte le attività di rete di un'applicazione software debbano essere rifiutate o consentite o vadano trattate in modo interattivo tramite la finestra di pop up *Evento di rete*.
Nella configurazione estesa della rubrica *Regole di applicazione*, è possibile definire per un'applicazione diversi filtri di pacchetto che vengono eseguiti come regole di applicazione specifiche.

8. Backup

Sono disponibili varie opzioni per creare un backup dei dati:

Backup tramite lo strumento di backup

Grazie agli strumenti di backup è possibile selezionare o creare un profilo di backup e avviare manualmente un backup per un profilo selezionato (vedere Backup tramite lo strumento di backup).

Backup tramite un job di backup in

Lo offre la possibilità di creare job di backup temporizzati o attivati da eventi. I job di backup vengono eseguiti automaticamente dallo . Questa procedura è l'ideale se di desidera salvare regolarmente dati specifici (vedere Backup tramite un job di backup in Scheduler).

9. Risoluzione di problemi, suggerimenti

9.1 Panoramica

In questo capitolo sono presenti indicazioni importanti per la risoluzione di problemi e ulteriori suggerimenti inerenti al prodotto Avira acquistato.

- Vedere capitolo Assistenza in caso di problemi
- Vedere capitolo Shortcut
- Vedere capitolo Centro di sicurezza di Windows

9.2 Assistenza in caso di problemi

Qui sono reperibili informazioni sulle cause e le soluzioni di eventuali problemi.

- Viene visualizzato il messaggio di errore *Il file di licenza non si apre*.
- Nel tentativo di avviare un aggiornamento apre un messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...*.
- Impossibile spostare o eliminare virus e malware.
- L'icona Tray mostra uno stato disattivato.
- Il computer è estremamente lento se effettuo il salvataggio di dati.
- Il mio Firewall segnala i servizi Avira Realtime Protection e Avira Mail Protection, se sono attivi
- Avira Mail Protection non funziona.
- Non è possibile effettuare connessioni a Internet in macchine virtuali se Avira FireWall è installato sul sistema operativo host e il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.
- La connessione Virtual Private Network (VPN) è bloccata se il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.
- Un'email inviata mediante una connessione TSL, è stata bloccata da Mail Protection.
- Webchat non funziona: non vengono visualizzati i messaggi chat.

Viene visualizzato il messaggio di errore: Il file di licenza non si apre.

Causa: il file è protetto.

- Per attivare la licenza non bisogna aprire il file, ma salvarlo nella directory del programma.

Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...* appare nel tentativo di avviare un aggiornamento.

Causa: la connessione Internet non è attiva. Pertanto, non può essere creato alcun collegamento al server Web in Internet.

- Provare se altri servizi Internet come WWW o l'email funzionano. Se non funzionano ripristinare la connessione Internet.

Causa: il server proxy non è raggiungibile.

- Verificare se sia cambiato il login per il server proxy e adattare eventualmente la propria configurazione.

Causa: il file update.exe non è ammesso dal proprio firewall.

- Assicurarsi che il file update.exe sia ammesso dal proprio firewall.

Altrimenti:

- Controllare le impostazioni nella configurazione (modalità esperto) in Generale > Aggiornamento.

Impossibile spostare o eliminare virus e malware.

Causa: il file è stato caricato da Windows ed è attivo.

- Aggiornare il prodotto Avira acquistato.
- Se si utilizza il sistema operativo Windows XP, disattivare il ripristino del sistema.
- Avviare il computer in modalità provvisoria.
- Avviare il programma Avira e la configurazione (Modalità esperto).
- Selezionare **System Scanner > Scansione > File > Tutti i file** e confermare la finestra con **OK**.
- Avviare una scansione su tutti i drive locali.
- Avviare il computer in modalità normale.
- Eseguire una scansione in modalità normale.
- Se non vengono rilevati altri virus e malware attivare il ripristino del sistema se è disponibile e deve essere utilizzato.

L'icona Tray mostra uno stato disattivato.

Causa: Il servizio Avira Realtime Protection è disattivato.

- Nel Control Center fare clic nella rubrica **Panoramica > Stato** nella sezione **Avira Realtime Protection** sul link **Attiva**.

Causa: Avira Realtime Protection è bloccato da un firewall.

- Nella configurazione del firewall definire un permesso generale per Avira Realtime Protection. Avira Realtime Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione internet. Lo stesso vale per Avira Mail Protection.

Altrimenti:

- Verificare la modalità di attivazione del servizio Avira Realtime Protection. Attiva eventualmente il servizio: selezionare in **Start > Impostazioni > Pannello di controllo**. Avviare il pannello di configurazione **Servizi** facendo doppio clic (in Windows 2000 e Windows XP l'applet servizi si trova nella sottodirectory *Gestione*). Cercare la voce *Avira Realtime Protection*. Come modalità di avviamento deve essere inserito `Automatico` e come stato `Avviato`. Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante **Avvia**. Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi.

Il computer diventa estremamente lento se eseguo un backup.

Causa: Avira Realtime Protection scansiona tutti i dati con i quali lavora il backup durante il processo di backup.

- Selezionare nella configurazione (modalità esperto) **Realtime Protection > Scansione > Eccezioni** e inserire il nome del processo del software di backup.

Il mio Firewall segnala i servizi Avira Realtime Protection e Avira Mail Protection, se sono attivi

Causa: La comunicazione di Avira Realtime Protection e Avira Mail Protection avviene mediante il protocollo Internet TCP/IP. Un firewall monitora tutte le connessioni mediante questo protocollo.

- Nella configurazione del firewall definire un permesso generale per Avira Realtime Protection e Avira Mail Protection. Avira Realtime Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione internet. Lo stesso vale per Avira Mail Protection.

Avira Mail Protection non funziona.

- ✓ Verificare la funzionalità di Avira Mail Protection sulla base delle seguenti checklist se si manifestano problemi con Avira Mail Protection.

Checklist

- ✓ Verificare se il client mail si registra mediante Kerberos, APOP o RPA sul server. Questi metodi di autenticazione attualmente non vengono supportati.
- ✓ Verificare se il client mail viene registrato mediante SSL (spesso chiamato anche TSL - Transport Layer Security) sul server. Avira Mail Protection non supporta alcun SSL e chiude pertanto le connessioni SSL crittografate. Se si desidera utilizzare le connessioni SSL crittografate senza la protezione di Avira Mail Protection, per la connessione occorre usare una porta diversa da quelle controllate da MailGuard. Le porte monitorate da Mail Protection possono essere configurate nella configurazione

in **Mail Protection > Scansione**.

✓ Il servizio Avira Mail Protection è attivo? Attiva eventualmente il servizio: selezionare in **Start > Impostazioni > Pannello di controllo**. Avviare il pannello di configurazione **Servizi** facendo doppio clic (in Windows 2000 e Windows XP l'applet servizi si trova nella sottodirectory *Gestione*). Cercare la voce *Avira Mail Protection*. Come modalità di avviamento deve essere inserito `Automatico` e come stato `Avviato`. Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante **Avvia**. Se viene visualizzato un messaggio di errore, verificare la *visualizzazione eventi*. Se non riesce, disinstallare completamente il prodotto Avira mediante **Start > Impostazioni > Pannello di controllo > Software**, riavviare il computer e, infine, installare nuovamente il prodotto Avira.

Generale

- Mediante SSL (Secure Sockets Layer) le connessioni crittografate POP3 (spesso definite anche TLS - Transport Layer Security) in questo momento non possono essere protette e vengono ignorate.
- L'autenticazione al server mail attualmente viene supportata solo con "password". "Kerberos" e "RPA" attualmente non sono supportati.
- Il prodotto Avira non cerca virus o programmi indesiderati all'invio di email.

> **Suggerimenti**
> Consigliamo di eseguire regolarmente gli aggiornamenti Microsoft per colmare le eventuali lacune in termini di sicurezza.

Non è possibile effettuare connessioni a Internet in macchine virtuali se Avira FireWall è installato sul sistema operativo host e il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.

Se Avira FireWall è installato su un computer dove viene gestito un sistema virtuale (ad esempio VMWare, Virtual PC, ecc.) questo blocca tutte le connessioni di rete del sistema virtuale se il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato. Se il livello di sicurezza è Basso FireWall reagisce conformemente alle aspettative.

Causa: il sistema virtuale emula una scheda di rete mediante software. Con l'emulazione i pacchetti di dati del sistema host sono incapsulati in pacchetti speciali (cosiddetti UDP) e reindirizzati mediante il gateway esterno al sistema host. In Avira FireWall vengono bloccati quelli provenienti dall'esterno a partire dal livello di sicurezza Medio.

Per gestire questo processo procedere come segue:

- Selezionare la rubrica **Protezione Online > FireWall** in Control Center.
- Fare clic sul link **Configurazione**.
- Viene visualizzata la finestra di dialogo *Configurazione*. Ci si trova nella rubrica di configurazione *Regole applicazione*.

- Attivare la **Modalità esperto**.
- Selezionare la rubrica di configurazione **Regole adattatore**.
- Fare clic su **Aggiungi**.
- In *Regola in entrata* selezionare **UDP**.
- Nella sezione Nome della regola indicare un **nome**.
- Fare clic su **OK**.
- Verificare se la regola gode di un livello di priorità superiore alla regola **Rifiuta tutti i pacchetti IP**.

> **Attenzione**
> Questa regola nasconde potenziali pericoli poiché si consentono i pacchetti UDP! Dopo il funzionamento del sistema virtuale tornare al precedente livello di sicurezza.

La connessione Virtual Private Network (VPN) è bloccata se il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.

Causa: il problema è l'ultima regola della catena**Rifiuta tutti i pacchetti IP**, che entra sempre in vigore quando un pacchetto non corrisponde a nessuna regola. I pacchetti inviati mediante software VPN vengono filtrati da questa regola dal momento che a causa della loro natura (cosiddetti pacchetti GRE) non ricadono in nessuna delle altre categorie.

- Sostituire la regola **Rifiuta tutti i pacchetti IP** con una nuova regola che rifiuta i pacchetti TCP e UDP. In questo modo esiste la possibilità che vengano consentiti pacchetti di altri protocolli.

Un'email inviata mediante una connessione TSL, è stata bloccata da Mail Protection.

Causa: Transport Layer Security (TLS: protocollo di codifica per la trasmissione dati su Internet) al momento non è supportato da Mail Protection. Per inviare l'email è possibile:

- utilizzare un'altra porta rispetto alla Porta 25 impegnata da SMTP. In questo modo si aggira la sorveglianza di Mail Protection.
- Rinunciare alla connessione codificata TSL e disattivare il supporto TSL nel client email.
- Disattivare (ignorare) il monitoraggio delle email in uscita da parte di Mail Protection nella configurazione in **MailGuard > Scansione**.

Webchat non funziona: i messaggi chat non vengono visualizzati, nel browser vengono caricati dei dati.

Questo fenomeno può verificarsi in chat che si basano sul protocollo HTTP con 'transfer-encoding=chunked'.

Causa: Web Protection controlla i dati inviati in modo completo alla ricerca di virus e programmi indesiderati prima che i dati siano caricati nel browser Web. Durante un trasferimento di dati con 'transfer-encoding=chunked' Web Protection non è in grado di rilevare la lunghezza dei messaggi o la quantità di dati.

- Nella configurazione impostare l'URL di Webchat come eccezione (vedere Configurazione: Web Protection > Eccezioni).

9.3 Shortcut

Le shortcut offrono la possibilità di navigare velocemente nel programma, richiamare singoli moduli e avviare azioni.

Di seguito viene presentata una panoramica delle shortcut presenti. Per maggiori informazioni sulla funzionalità e disponibilità consultare il capitolo corrispondente della guida.

9.3.1 Nelle finestre di dialogo

Shortcut	Descrizione
Ctrl + Tab **Ctrl + Page down**	Navigazione in Control Center Passa alla rubrica successiva.
Ctrl + Shift + Tab **Ctrl + Page down**	Navigazione in Control Center Passa alla rubrica precedente.
← ↑ → ↓	Navigazione nelle rubriche di configurazione Evidenzia con il mouse una rubrica di configurazione.
Tab	Passa all'opzione successiva o al successivo gruppo di opzioni.
Shift + Tab	Passa all'opzione precedente o al precedente gruppo di opzioni.
← ↑ → ↓	Effettua una modifica tra le opzioni di un menu a tendina selezionate o tra più opzioni in un gruppo di opzioni.

Barra spaziatrice	Attiva o disattiva una casella di controllo se l'opzione attiva è una casella di controllo.
Alt + lettera sottolineata	Seleziona l'opzione o esegui il comando.
Alt + ↓ **F4**	Apri il menu a tendina selezionato.
Esc	Chiudi il menu a tendina selezionato. Annulla il comando e chiudi la finestra di dialogo.
Invio	Esegui comando per l'opzione o il pulsante attivo.

9.3.2 Nella Guida in linea

Shortcut	Descrizione
Alt + barra spaziatrice	Visualizza il menu del sistema.
Alt + Tab	Passa dalla Guida in linea ad altre finestre aperte.
Alt + F4	Chiudi la Guida in linea.
Shift+ F10	Visualizza menu contestuali della Guida in linea.
Ctrl + Tab	Passa alla rubrica successiva nella finestra di navigazione.
Ctrl + Shift + Tab	Passa alla rubrica precedente nella finestra di navigazione.
Page up	Passa all'argomento che è visualizzato sopra l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page down	Passa all'argomento che è visualizzato sotto l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.

Page up **Page down**	Sfoglia le voci su un argomento.

9.3.3 In Control Center

Generale

Shortcut	Descrizione
F1	Visualizza Guida in linea
Alt + F4	Chiudi Control Center
F5	Aggiorna visualizzazione
F8	Apri configurazione
F9	Avvia aggiornamento

Rubrica **Scansiona**

Shortcut	Descrizione
F2	Rinomina il profilo selezionato
F3	Avvia la scansione con il profilo selezionato
F4	Crea collegamento sul desktop per il profilo selezionato
Agg	Crea nuovo profilo
Canc	Elimina profilo selezionato

Rubrica **FireWall**

Shortcut	Descrizione
Invio	Proprietà

Rubrica **Quarantena**

Shortcut	Descrizione
F2	Riscansiona l'oggetto
F3	Ripristina l'oggetto
F4	Invia l'oggetto
F6	Ripristina l'oggetto in...
Invio	Proprietà
Agg	Aggiungi file
Canc	Elimina l'oggetto

Rubrica **Scheduler**

Shortcut	Descrizione
F2	Modifica job
Invio	Proprietà
Agg	Inserisci nuovo job
Canc	Elimina job

Rubrica **Report**

Shortcut	Descrizione
F3	Visualizza il file di report
F4	Stampa il file di report
Invio	Mostra il report
Canc	Elimina il report

Rubrica **Eventi**

Shortcut	Descrizione
F3	Esporta evento
Invio	Mostra evento
Canc	Elimina evento

9.4 Centro di sicurezza di Windows

- a partire da Windows XP Service Pack 2 -

9.4.1 Generale

Il Centro sicurezza di Windows verifica lo stato di un computer dal punto di vista della sicurezza.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro sicurezza invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer.

9.4.2 Il Centro sicurezza di Windows e il prodotto Avira acquistato

Firewall

È possibile ricevere dal Centro sicurezza le seguenti informazioni relative al firewall:

- Firewall AKTIV / Firewall attivo
- Firewall INAKTIV / Firewall non attivo

Firewall AKTIV / Firewall attivo

Dopo l'installazione del prodotto Avira e la chiusura del firewall di Windows si riceve il seguente avviso:

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo

Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo

Modifica impostazioni Centro operativo

Modifica impostazioni di Controllo dell'account utente

Visualizza messaggi archiviati

Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi

Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)

Avira Desktop non è aggiornato.

Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati

Aggiorna

Recuperare un altro programma antispyware online

Protezione da virus (Importante)

Avira Desktop non è aggiornato.

Disattiva i messaggi relativi a: protezione da virus

Aggiorna ora

Recuperare un altro programma antivirus online

Windows Update

Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.

Disattiva i messaggi relativi a: Windows Update

Cambia impostazioni...

Manutenzione

Imposta backup

Il backup dei file non è in corso.

Disattiva i messaggi relativi a: Windows Backup

Imposta backup

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:

Risoluzione dei problemi
Trova e risolve i problemi

Ripristino
Ripristina una condizione precedente del computer

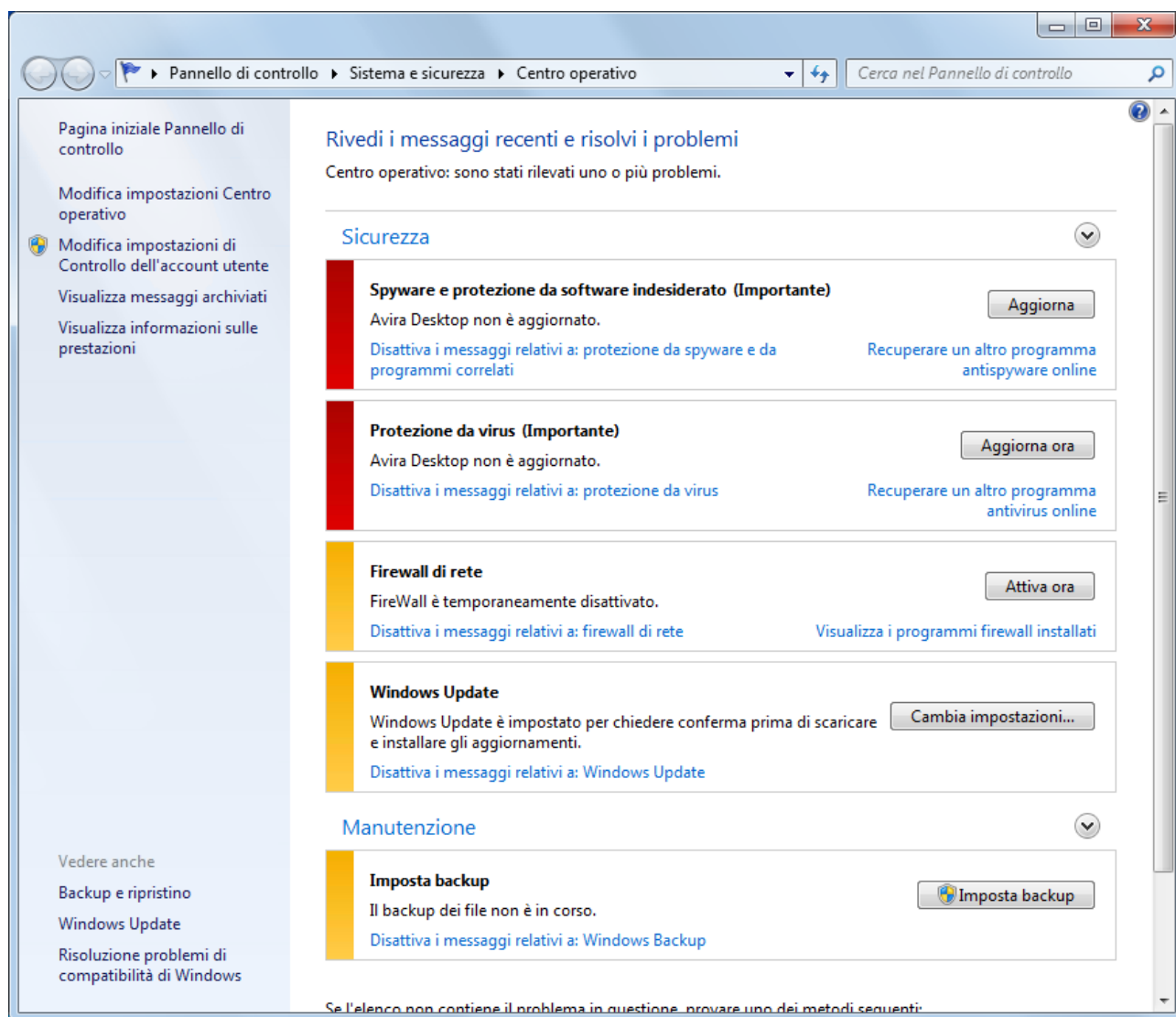
Vedere anche

Backup e ripristino

Windows Update

Risoluzione problemi di compatibilità di Windows

Firewall INATTIVO/Firewall non attivo

Si riceve il seguente messaggio se si disattiva il FireWall di Avira:

Suggerimenti
È possibile attivare o disattivare il FireWall di Avira tramite Stato nel Control Center.

Attenzione
Se viene disattivato il FireWall di Avira, il computer non è più protetto da accessi non autorizzati dalla rete o da Internet.

Software di protezione antivirus/Protezione da software dannoso

È possibile ricevere i seguenti avvisi dal Centro sicurezza di Windows in relazione alla protezione antivirus.

- Protezione antivirus NON TROVATA
- Protezione antivirus NON AGGIORNATA

- Protezione antivirus ATTIVA
- Protezione antivirus INATTIVA
- Protezione antivirus NON MONITORATA

Protezione antivirus NON TROVATA

Questo avviso del Centro sicurezza di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

« Tutti gli elementi del Pannello di controllo ▸ Centro operativo
Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo
Modifica impostazioni Centro operativo
Modifica impostazioni di Controllo dell'account utente
Visualizza messaggi archiviati
Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi
Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)
Windows Defender è disattivato.
Attiva ora
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Recuperare un altro programma antispyware online

Protezione da virus (Importante)
Impossibile trovare software antivirus installato nel computer.
Trova programma online
Disattiva i messaggi relativi a: protezione da virus

Firewall di rete (Importante)
Windows Firewall è disattivato o configurato in modo errato.
Attiva ora
Disattiva i messaggi relativi a: firewall di rete
Recuperare un altro programma firewall online

Windows Update
Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.
Cambia impostazioni...
Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup
Il backup dei file non è in corso.
Imposta backup
Disattiva i messaggi relativi a: Windows Backup

Vedere anche
Backup e ripristino
Windows Update
Risoluzione problemi di compatibilità di Windows

Suggerimenti
Installare il prodotto Avira sul computer per proteggerlo da virus e altri programmi indesiderati!

Protezione antivirus NON AGGIORNATA

Se si possiede Windows XP Service Pack 2 o Windows Vista e si installa successivamente il prodotto Avira oppure si installa Windows XP Service Pack 2 o Windows Vista su un sistema su cui è già installato il prodotto Avira, si riceve il seguente messaggio:

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo
Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo
Modifica impostazioni Centro operativo
Modifica impostazioni di Controllo dell'account utente
Visualizza messaggi archiviati
Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi
Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)
Avira Desktop non è aggiornato.
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Aggiorna
Recuperare un altro programma antispyware online

Protezione da virus (Importante)
Avira Desktop non è aggiornato.
Disattiva i messaggi relativi a: protezione da virus
Aggiorna ora
Recuperare un altro programma antivirus online

Windows Update
Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.
Disattiva i messaggi relativi a: Windows Update
Cambia impostazioni...

Manutenzione

Imposta backup
Il backup dei file non è in corso.
Disattiva i messaggi relativi a: Windows Backup
Imposta backup

Vedere anche
Backup e ripristino
Windows Update
Risoluzione problemi di compatibilità di Windows

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:

Risoluzione dei problemi
Trova e risolve i problemi

Ripristino
Ripristina una condizione precedente del computer

Suggerimenti
Per far sì che il Centro sicurezza di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Protezione antivirus ATTIVA

Dopo l'installazione del prodotto Avira e un susseguente aggiornamento, si riceve la seguente nota:

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo
Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo
Modifica impostazioni Centro operativo
Modifica impostazioni di Controllo dell'account utente
Visualizza messaggi archiviati
Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi
Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)
Avira Desktop non è aggiornato.
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Aggiorna
Recuperare un altro programma antispyware online

Protezione da virus (Importante)
Avira Desktop non è aggiornato.
Disattiva i messaggi relativi a: protezione da virus
Aggiorna ora
Recuperare un altro programma antivirus online

Windows Update
Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.
Disattiva i messaggi relativi a: Windows Update
Cambia impostazioni...

Manutenzione

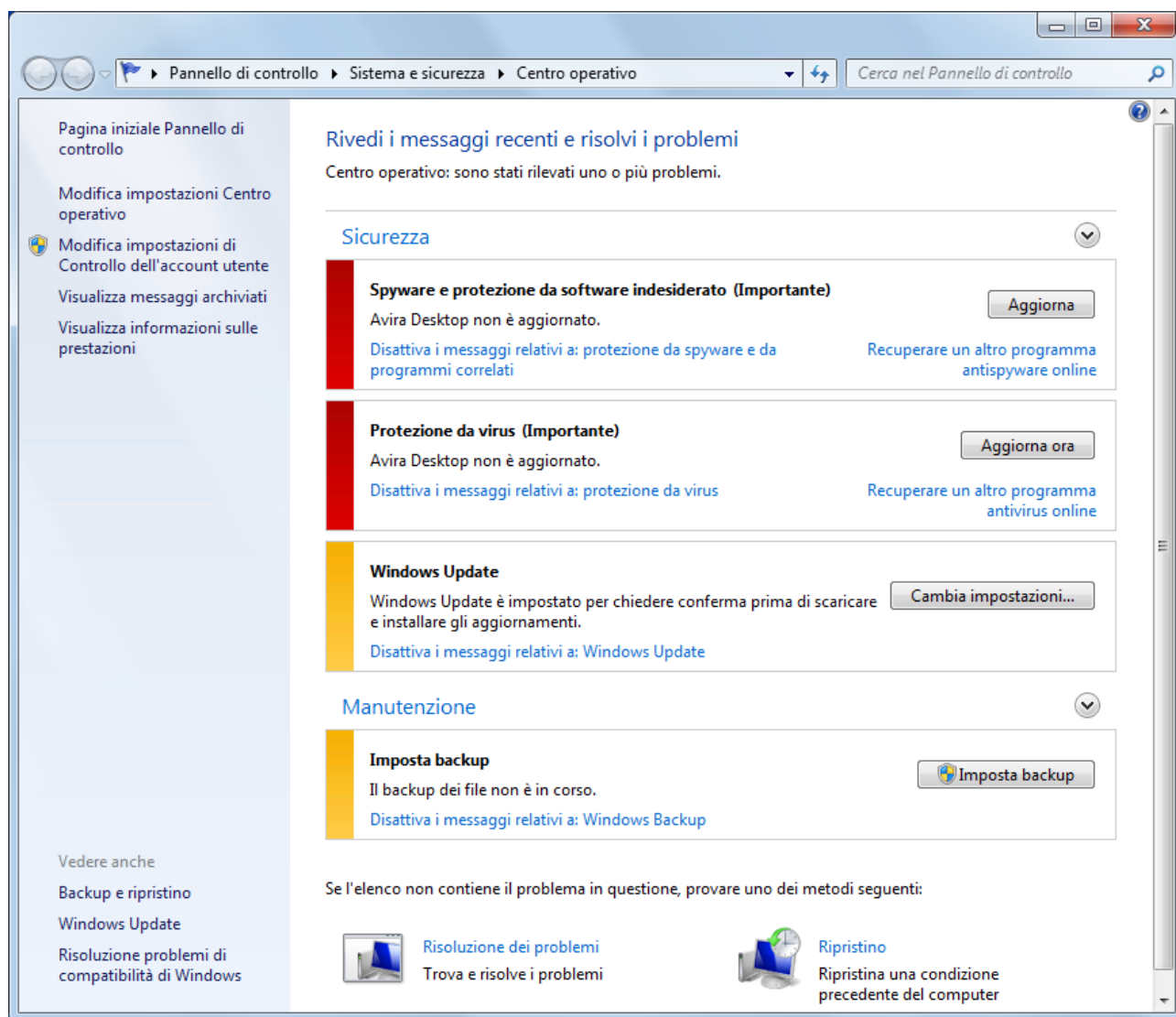
Imposta backup
Il backup dei file non è in corso.
Disattiva i messaggi relativi a: Windows Backup
Imposta backup

Vedere anche
Backup e ripristino
Windows Update
Risoluzione problemi di compatibilità di Windows

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:
Risoluzione dei problemi
Trova e risolve i problemi
Ripristino
Ripristina una condizione precedente del computer

Il prodotto Avira è aggiornato e Avira Realtime Protection è attivo.

Protezione antivirus INATTIVA

Si riceve la seguente nota se si disattiva Avira Realtime Protection o si arresta il servizio.

Suggerimenti
È possibile attivare e disattivare Avira Realtime Protection nella rubrica Panoramica > Stato del Control Center. Inoltre Avira Realtime Scanner viene riconosciuto come attivato quando l'ombrellino rosso nella barra delle applicazioni è aperto.

Protezione antivirus NON MONITORATA

Si riceve il seguente messaggio dal Centro sicurezza di Windows poiché si è optato per l'automonitoraggio del software antivirus.

Suggerimenti
La funzione non è supportata da Windows Vista.

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo
Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo
Modifica impostazioni Centro operativo
Modifica impostazioni di Controllo dell'account utente
Visualizza messaggi archiviati
Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi
Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)
Avira Desktop non è aggiornato.
Aggiorna
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Recuperare un altro programma antispyware online

Protezione da virus (Importante)
Avira Desktop non è aggiornato.
Aggiorna ora
Disattiva i messaggi relativi a: protezione da virus
Recuperare un altro programma antivirus online

Windows Update
Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.
Cambia impostazioni...
Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup
Il backup dei file non è in corso.
Imposta backup
Disattiva i messaggi relativi a: Windows Backup

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:

Risoluzione dei problemi
Trova e risolve i problemi

Ripristino
Ripristina una condizione precedente del computer

Vedere anche
Backup e ripristino
Windows Update
Risoluzione problemi di compatibilità di Windows

Suggerimenti

Il Centro sicurezza di Windows è supportato dal prodotto Avira acquistato. È possibile attivare questa opzione in ogni momento con il pulsante **Consigli...**.

Suggerimenti

Anche se sono installati Windows XP Service Pack 2 o Windows Vista, si ha comunque bisogno di una soluzione antivirus. Sebbene Windows XP Service Pack 2 controlli il software antivirus non ha alcuna funzione antivirus. L'utente non sarebbe protetto contro virus e malware senza una soluzione antivirus aggiuntiva!

10. Virus e altro

10.1 Categorie di minacce

Adware

Con Adware si designa un software che mostra all'utente i banner e i pop up pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Il prodotto Avira riconosce Adware. Se nella configurazione in Categorie delle minacce l'opzione **Adware** è attivata, si riceve un avviso quando il prodotto Avira rileva tale software.

Adware/Spyware

Software che visualizza messaggi pubblicitari o che invia i dati personali dell'utente, spesso a sua insaputa, a terzi e che risulta quindi indesiderato.

Il prodotto Avira riconosce "Adware/Spyware". Se nella configurazione in Categorie delle minacce l'opzione **Adware/Spyware** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Applicazione

Con la denominazione "Applicazione" si intende un'applicazione il cui utilizzo può essere rischioso o la cui origine è dubbia.
Il prodotto Avira riconosce l'"Applicazione" (APPL). Se nella configurazione in Categorie delle minacce l'opzione **Applicazione** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira rileva un tale comportamento.

Software di gestione Backdoor

Per prelevare dati o manipolare il sistema viene inserito "dalla porta posteriore" un programma server backdoor senza che l'utente se ne accorga. Questo programma può essere gestito da terzi mediante Internet o la rete con un software di gestione backdoor (Client).
Il prodotto Avira riconosce il "Software di gestione Backdoor". Se nella configurazione in Categorie delle minacce l'opzione **Software di gestione Backdoor** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

File con estensioni nascoste

File eseguibili che occultano la propria estensione in modo sospetto. Il metodo dell'occultamento viene spesso utilizzato dai malware.

Il prodotto Avira riconosce i "file con estensioni nascoste". Se nella configurazione in Categorie delle minacce l'opzione **File con estensioni nascoste** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programma di selezione a pagamento

Alcuni servizi offerti in Internet sono a pagamento. In Germania la fatturazione avviene per programmi di selezione con i numeri 0190/0900 (in Austria e Svizzera con i numeri 09x0; in Germania a medio termine passerà ai numeri 09x0). Installati sul computer, questi programmi - in breve dialer - garantiscono la creazione della connessione mediante i numeri Premium-Rate, la cui tariffa può variare enormemente.

La commercializzazione di contenuti online mediante la bolletta telefonica è legale e può essere vantaggiosa per l'utente. I dialer seri non hanno alcun dubbio sul fatto che il cliente sia consapevole e lo utilizzi in modo avveduto. Tali contenuti si installano sul computer dell'utente solo se l'utente dà la propria approvazione, espressa sulla base di un'etichettatura ben riconoscibile o di una richiesta univoca e chiara. La creazione della connessione di programmi dialer seri viene visualizzata in maniera chiara e non ambigua. Inoltre, i dialer seri informano l'utente in maniera esatta e precisa sui costi correlati.

Purtroppo però esistono dialer che si installano senza farsi notare, in maniera dubbia o addirittura fraudolenta. Sostituiscono, ad esempio, la connessione standard dial up dell'utente di Internet all'ISP (Internet-Service-Provider) e a ogni connessione selezionano numeri a pagamento spesso estremamente costosi, come i numeri 0190/0900. L'utente interessato nota dalla bolletta successiva che si è installato un programma dialer indesiderato che si connette a ogni accesso a Internet ai numeri a pagamento 0190/0900 - determinando così una bolletta estremamente cara.

Per proteggersi da programmi di selezione non desiderati e a pagamento (dialer 0190/0900), consigliamo di rivolgersi direttamente al proprio gestore telefonico per bloccare questo tipo di numeri.

Di default, il prodotto Avira riconosce i programmi di selezione a pagamento a lui noti.

Se nella configurazione di Categorie delle minacce l'opzione **Programma di selezione a pagamento** è attivata con un segno di spunta, in caso di rilevamento di un programma di selezione a pagamento si riceve un messaggio di avviso. Si ha quindi la possibilità di eliminare facilmente gli eventuali dialer indesiderati per i numeri 0190/0900. Se si tratta di un programma di selezione a pagamento voluto, si può dichiarare un file da escludere che non verrà più scansionato in futuro.

Phishing

Il phishing, anche noto come "brand spoofing" è una forma raffinata di furto dei dati per i clienti o i potenziali clienti di provider Internet, banche, servizi di online banking, enti di registrazione.
Con la trasmissione dell'indirizzo email in Internet, la compilazione di moduli online, la partecipazione a newsgroup o siti web è possibile che vengano sottratti i dati dai cosiddetti

"Internet crawling spiders" e utilizzati senza consenso per effettuare frodi o altre attività illegali.

Il prodotto Avira riconosce il "phishing". Se nella configurazione in Categorie delle minacce l'opzione **Phishing** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira rileva un tale comportamento.

Programmi che violano la privacy dell'utente

Software che minano la sicurezza del sistema, causano funzioni di programma non desiderate, violano la sfera privata o spiano il comportamento dell'utente e che sono quindi generalmente indesiderati.

Il prodotto Avira riconosce il "software Security Privacy Risk". Se nella configurazione in Categorie delle minacce l'opzione **Programmi che violano la privacy dell'utente** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programmi ludici

I programmi ludici possono inorridire qualcuno o divertire tutti, senza essere dannosi o moltiplicarsi. La maggior parte delle volte il computer dopo il richiamo del programma ludico inizia a far suonare una melodia o a visualizzare qualcosa di insolito sullo schermo. Esempi di programmi ludici sono le lavatrici nel drive del floppy disk (DRAIN.COM) o il divoraschermo (BUGSRES.COM).

Ma attenzione! Tutte le manifestazioni di un programma ludico potrebbero anche essere prodotte da un virus o un trojan. L'effetto minimo sull'utente è uno spavento ma si può anche andare nel panico per la paura dei danni che possono verificarsi.

Il prodotto Avira è in grado di riconoscere i programmi ludici mediante un'estensione delle proprie routine di scansione ed eventualmente di eliminare il programma indesiderato. Se nella configurazione in Categorie delle minacce l'opzione **Programmi ludici** è attivata con un segno di spunta, si viene informati sui relativi rilevamenti.

Giochi

I giochi per computer devono esistere, ma non necessariamente sul luogo di lavoro (ad eccezione a volte della pausa pranzo). Tuttavia i dipendenti delle aziende e i collaboratori degli enti pubblici spesso usano i giochi. Su Internet sono disponibili moltissimi giochi. Anche i giochi per email stanno conoscendo una rapida espansione: dai semplici scacchi fino a "battaglia navale" esistono numerose varianti: i giochi vengono inviati per email ai partner e accettati da questi ultimi.

Alcune ricerche hanno dimostrato che il tempo durante l'orario lavorativo dedicato ai giochi per computer sta assumendo proporzioni rilevanti. Pertanto è comprensibile che sempre più aziende prendano in considerazione la possibilità di eliminare i giochi dai computer utilizzati per lavoro.

Il prodotto Avira riconosce i giochi per computer. Se nella configurazione in Categorie delle minacce l'opzione **Giochi** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento. Il gioco è finito nel vero senso della parola visto che è possibile escluderlo facilmente.

Software ingannevole

Conosciuto anche come "Scareware" (programma che fa spavento dall'inglese "to scare") o "Rogueware" (programma perfido o falso antivirus), definisce software fraudolento, che simula infezioni causate da virus e minacce, e assomiglia in modo sorprendente ai software antivirus professionali. Scareware è progettato per rendere insicuro o impaurire l'utente. La vittima cade nel trabocchetto e si crede minacciata, per cui le viene proposta, spesso a pagamento, l'eliminazione di un pericolo inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile un'attacco vero e proprio.

Se nella configurazione di Categorie delle minacce l'opzione **Software ingannevole** è attivata con un segno di spunta, in caso di rilevamento di scareware si riceve un messaggio di avviso.

Strumento di compressione runtime insolito

I file compressi con un programma zip runtime insolito possono essere identificati come sospetti.

Il prodotto Avira riconosce "Strumento di compressione runtime insolito". Se nella configurazione in Categorie delle minacce l'opzione **Strumento di compressione runtime insolito (PCK)** è attivata, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

10.2 Virus e altri malware

Adware

Con Adware si designa un software che mostra all'utente i banner e i pop up pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Backdoor

Un Backdoor (italiano: porta posteriore) permette, aggirando la tutela all'accesso, di ottenere l'accesso a un computer.

Un programma in esecuzione di nascosto permette a un aggressore di godere di diritti pressoché illimitati. Con l'aiuto del backdoor i dati personali dell'utente possono essere

spiati. I backdoor però vengono utilizzati soprattutto per installare altri virus o worm sul sistema infetto.

Virus dei record di avvio

Il record di avvio e il record master di avvio degli hard disk vengono inficiati di preferenza da virus dei record di avvio, che sovrascrivono informazioni importanti all'avvio del sistema. Una delle conseguenze spiacevoli: il sistema operativo non può più essere caricato...

Bot-Net

Per Bot-Net si intende una rete di PC gestibile a distanza (in Internet), composta da bot che comunicano l'uno con l'altro. Questo controllo si raggiunge con virus e trojan che inficiano il computer e poi aspettano indicazioni senza apportare danni al computer intaccato. Queste reti possono essere utilizzare per la diffusione di spam, attacchi DDoS, ecc., talvolta senza che gli utenti del PC si accorgano di alcunché. Il potenziale principale dei Bot-Net è quello di poter raggiungere reti di migliaia di computer, la cui portata salta gli accessi a Internet.

Exploit

Un Exploit (lacuna di sicurezza) è un programma del computer o uno script che sfrutta le debolezze specifiche o le funzioni errate di un sistema operativo o del programma. Una forma di Exploit sono gli attacchi da Internet con l'aiuto di pacchetti di dati manipolati, che sfruttano le debolezze nel software di rete. Con l'utilizzo di alcuni programmi che si introducono clandestinamente si ottiene un più ampio accesso.

Hoaxes (inglese: hoax - scherzo, burla)

Da un paio di anni gli utenti ricevono avvisi di virus che potrebbero diffondersi per email in Internet o in altre reti. Questi avvisi vengono distribuiti per email con la richiesta di inoltrarli a quanti più colleghi e utenti possibili per metterli in guardia sul "pericolo".

Honeypot

Un Honeypot (pentola di miele) è un servizio installato in una rete (programma o server). Esso ha il compito di monitorare una rete e registrare gli attacchi. Questo servizio è sconosciuto all'utente legittimo e quindi non viene mai toccato. Quando un aggressore cerca punti di debolezza in una rete e prende in considerazione i servizi offerti da un Honeypot viene registrato e viene emesso un allarme.

Macrovirus

I macrovirus sono piccoli programmi che sono scritti nella lingua delle macro di un'applicazione (ad esempio WordBasic in WinWord 6.0) e normalmente potrebbero diffondersi all'interno di documenti di questa applicazione. Essi vengono pertanto chiamati anche virus dei documenti. Per renderli attivi è necessario avviare l'applicazione corrispondente ed eseguire una delle macro infette. Diversamente dai virus "normali" i macrovirus non riguardano file eseguibili, ma documenti dell'applicazione host.

Pharming

Il pharming è una manipolazione del file host dei browser Web, per reindirizzare richieste dei siti Web falsificati. Si tratta di una rielaborazione del classico phishing. I truffatori che si servono del pharming godono di grandi quantità di server sui quali vengono archiviati i siti Web falsificati. Il pharming si è consolidato come iperonimo per diversi tipi di attacchi al DNS. In caso di manipolazione del file host con l'ausilio di un trojan o un virus viene effettuata una manipolazione del sistema. La conseguenza è che sono richiamabili solo siti Web falsificati da questo sistema, se l'indirizzo Web viene inserito correttamente.

Phishing

Phishing significa letteralmente pescare dati personali degli utenti di Internet. Il phisher invia generalmente alla vittima lettere aventi valore ufficiale, come ad esempio email che veicolano informazioni sensibili, soprattutto nomi utenti e password o PIN e TAN di accessi all'Online-Banking, approfittando della sua buona fede. Con i dati di accesso rubati il phisher assume l'identità della vittima e conduce operazioni a suo nome. Una cosa è certa: le banche e le assicurazioni non chiedono mai di inviare numeri di carte di credito, PIN, TAN o altri dati di accesso per email, SMS o telefonicamente.

Virus polimorfi

I veri campioni del mimetismo e del travestimento sono i virus polimorfi. Modificano i codici di programmazione e sono pertanto difficili da riconoscere.

Virus di programma

Un virus del computer è un programma che ha la capacità, una volta richiamato, di agganciarsi in qualche modo ad altri programmi e, da tale posizione, di inficiare il sistema. I virus si diffondono quindi in contrasto alle bombe logiche e ai trojan stessi. Al contrario di un worm, un virus ha bisogno di un programma estraneo ospite in cui archiviare il proprio codice virulento. Normalmente, la funzionalità del programma ospite non viene modificata.

Rootkits

Per Rootkit si intende un insieme di strumenti software che vengono installati su un computer dopo un'irruzione per nascondere il login dell'intruso, nascondere processi e registrare dati - in linea generale: per rendersi invisibile. I rootkit tentano di aggiornare i programmi spia già installati e di installare nuovamente gli spyware eliminati.

Virus di script e worm

Questi virus sono estremamente semplici da programmare e in poche ore si diffondono per email a livello globale, premesso che siano presenti tecniche ad hoc.

I virus di script e i worm utilizzano la lingua degli script, come ad esempio Javascript, VBScript ecc., per inserirsi in altri nuovi script o per diffondersi mediante il richiamo di funzioni del sistema operativo. Spesso ciò avviene tramite email o mediante lo scambio di file (documenti).

Il worm è un programma che non intacca alcun documento ospite. I worm non possono quindi divenire una componente di altri programmi. I worm rappresentano spesso l'unica possibilità di introdursi clandestinamente su sistemi dotati di provvedimenti restrittivi legati alla sicurezza.

Spyware

Gli spyware sono i cosiddetti programmi spia che inviano dati personali dell'utente a terzi senza che questi ne siano a conoscenza e senza l'approvazione del produttore del software. I programmi spyware servono soprattutto ad analizzare la navigazione in Internet e a introdurre banner o pop up pubblicitari in maniera mirata.

Cavalli di Troia (in breve trojan)

I trojan sono sempre più diffusi. Così vengono definiti i programmi che pretendono di avere una funzione precisa; dopo il loro avvio, tuttavia, mostrano il loro vero volto ed eseguono altre funzioni che hanno per lo più effetti distruttivi. I trojan non possono moltiplicarsi da soli e in questo si differenziano dai virus e dai worm. La maggior parte di loro ha un nome interessante (SEX.EXE o STARTME.EXE), che ha la funzione di spingere l'utente a eseguire il trojan. Subito dopo l'esecuzione diventano attivi e formattano, ad esempio, l'hard disk. Un tipo particolare di trojan è il dropper, che "lascia cadere" i virus, ovvero li installa nel sistema del computer.

Software ingannevole

Conosciuto anche come "Scareware" (programma che fa spavento dall'inglese "to scare") o "Rogueware" (programma perfido o falso antivirus), definisce software fraudolento, che simula infezioni causate da virus e minacce, e assomiglia in modo sorprendente ai software antivirus professionali. Scareware è progettato per rendere insicuro o impaurire

l'utente. La vittima cade nel trabocchetto e si crede minacciata, per cui le viene proposta, spesso a pagamento, l'eliminazione di un pericolo inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile un'attacco vero e proprio.

Zombie

Un PC zombie è un calcolatore che è intaccato da programmi malware e permette all'hacker di abusare del computer mediante la gestione a distanza per fini criminali. Il PC infetto lancia il comando, ad esempio, di attacchi di Denial-of-Service- (DoS) o invia spam o email di phishing.

11. Info e Service

In questo capitolo si ottengono informazioni sui modi in cui è possibile tenersi in contatto con noi.

- Vedere capitolo Indirizzo di contatto
- Vedere capitolo Supporto tecnico
- Vedere capitolo File sospetto
- Vedere capitolo Comunicare un falso allarme
- Vedere capitolo Un suo feedback per una maggiore sicurezza

11.1 Indirizzi di contatto

Siamo a disposizione del cliente qualora avesse domande o suggerimenti sul mondo dei prodotti Avira. I nostri indirizzi dove contattarci sono disponibili in Guida in linea > Informazioni su Avira Internet Security 2012.

11.2 Supporto tecnico

Il supporto Avira si rivolge all'utente in modo affidabile e serve a rispondere alle sue domande o a risolvere un problema tecnico.

Sul nostro sito Web l'utente può riferire tutte le informazioni utili per il nostro ampio servizio di supporto:
http://www.avira.it/premium-suite-support

Per poter ricevere aiuto nel modo migliore e più veloce possibile l'utente deve prendere in considerazione le seguenti informazioni:

- **Dati sulla licenza**. Essi si trovano sull'interfaccia del programma nella voce di menu **Guida in linea > Informazioni su Avira Internet Security 2012 > Informazioni sulla licenza**. Vedere Informazioni sulla licenza.
- **Informazioni sulla versione**. Esse si trovano sull'interfaccia del programma nella voce di menu **Guida in linea > Informazioni su Avira Internet Security 2012 > Informazioni sulla versione**. Vedere Informazioni sulla versione.
- **Versione del sistema operativo** e service pack eventualmente installati.
- **I pacchetti software installati**, ad esempio software antivirus di altri produttori.
- **Messaggi precisi** del programma o del file di report.

11.3 File sospetto

I virus che non possono essere riconosciuti o eliminati dai nostri prodotti così come i file sospetti possono essere inviati a noi. A tale scopo sono disponibili diverse modalità di invio.

- Selezionare il file nel Gestore della quarantenadel Control Center e selezionare la voce Invia file mediante il menu contestuale o i pulsanti corrispondenti.
- Allegare il file desiderato compresso (WinZIP, PKZip, Arj, ecc.) ad un'email e inviarlo al seguente indirizzo:
  virus-premium-suite@avira.it
  Poiché alcuni gateway email operano con software antivirus, si prega di proteggere il/i file con una password (non dimenticare di comunicare anche la password).
- In alternativa è possibile inviare il file sospetto mediante la nostra pagina web:
  http://www.avira.it/sample-upload

11.4 Comunicare un falso allarme

Se si ritiene che il proprio prodotto Avira abbia segnalato un rilevamento in un file che tuttavia con ogni probabilità è "pulito", si prega di inviare tale file compresso (WinZIP, PKZIP, Arj, ecc.) per email come allegato al seguente indirizzo:
virus-premium-suite@avira.it

Poiché alcuni Email-Gateways operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

11.5 Un suo Feedback per una maggiore sicurezza

Per Avira la sicurezza degli utenti è al primo posto. Pertanto non disponiamo solamente di un team di esperti, a cui viene sottoposta ogni singola soluzione di Avira e ogni aggiornamento prima della pubblicazione dei test di sicurezza e qualità. Consigliamo di prendere seriamente le note su eventuali punti di debolezza rilevanti per la sicurezza e le si tratti chiaramente.

Se si ritiene che esista una lacuna rilevante per la sicurezza in uno dei nostri prodotti inviare un'email al seguente indirizzo:

vulnerabilities-premium-suite@avira.it

12. Riferimento: Opzioni di configurazione

Il riferimento della configurazione elenca le opzioni di configurazione disponibili.

12.1 System Scanner

La rubrica **System Scanner** della configurazione è dedicata alla configurazione della scansione diretta, ovvero alla scansione su richiesta. (Opzioni disponibili solo in Modalità esperto).

12.1.1 Cerca

Qui si può definire la procedura standard della routine di scansione durante una scansione diretta (opzioni disponibili solo in Modalità esperto). Se si seleziona una determinata directory da controllare durante la scansione diretta, il System Scanner esegue i controlli in base alla configurazione:

- con una determinata prestazione di scansione (priorità),
- anche sui record di avvio e nella memoria principale,
- su tutti i file o i file selezionati nella directory.

File

Il System Scanner può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione. Il filtro non viene utilizzato.

> **Suggerimenti**
> Se **Tutti i file** è attivo, il pulsante **Estensioni dei file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il prodotto Avira decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza lista estensione file**, ma molto più sicura poiché i controlli non sono effettuati solamente sulla base delle estensioni dei file. Questa opzione è attivata di default ed è consigliata.

Suggerimenti
Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non può essere scelto.

Utilizza la lista delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**.

Suggerimenti
Se questa opzione è attivata e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza elenco estensioni file"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Suggerimenti
Prestare attenzione al fatto che l'elenco standard può variare da versione a versione.

Impostazioni aggiuntive

Scansiona settori di avvio dei drive

Se l'opzione è attivata, il System Scanner controlla i record di avvio dei drive selezionati durante la scansione diretta. Questa opzione è attivata di default.

Scansione dei record master di avvio

Se l'opzione è attivata, il System Scanner controlla i record master di avvio degli/dell'hard disk utilizzati/o nel sistema.

Ignora i file offline

Se l'opzione è attivata, durante la scansione diretta i cosiddetti file offline vengono completamente ignorati. Ciò significa che in questi file non viene controllata la presenza di virus e programmi indesiderati. I file offline sono quei file che sono stati archiviati fisicamente dall'hard disk, per es. su un nastro, mediante il cosiddetto sistema gerarchico di gestione della memoria. Questa opzione è attivata di default.

Controllo di integrità dei file di sistema

Se l'opzione è attivata, i principali file di sistema Windows vengono sottoposti a una verifica particolarmente sicura durante ogni scansione diretta per verificare la presenza di modifiche dovute a malware. Se viene individuato un file modificato, questo viene segnalato come rilevamento sospetto. La funzionalità occupa molta memoria. Per questo motivo l'opzione è disattivata di default.

Suggerimenti
L'opzione è disponibile solo a partire da Windows Vista.

Suggerimenti
Se si utilizzano strumenti di terzi, si modificano i file di sistema o si personalizza la schermata di avvio, questa opzione non deve essere utilizzata. Questi strumenti sono, ad esempio, i cosiddetti skinpack, TuneUp Utilities o Vista Customization.

Scansione ottimizzata

Se l'opzione è attivata, la capacità del processore viene utilizzata in modo ottimale durante la scansione con il System Scanner. Per motivi di performance, in caso di scansione ottimale, la funzione di report si verifica al massimo a un livello standard.

Suggerimenti
L'opzione è disponibile solo per computer multiprocessore,

Seguire link simbolici

Se l'opzione è attivata, il System Scanner esegue una scansione di tutti i collegamenti simbolici nel profilo di ricerca o nelle directory selezionate, allo scopo di scansionare i file collegati alla ricerca di virus e malware.

Suggerimenti
L'opzione non comprende i collegamenti (shortcut), bensì si riferisce esclusivamente ai link simbolici (generati con mklink.exe) o ai punti di giunzione (generati con junction.exe), presenti in modalità trasparente nel file system.

Scansione rootkit all'avvio

Se l'opzione è attivata, il System Scanner verifica con una scansione all'avvio la directory di sistema Windows tramite una procedura rapida per verificare la presenza di eventuali rootkit attivi. Questa procedura non verifica se nel computer vi sono rootkit

attivi così dettagliatamente come il profilo di ricerca "**Cerca rootkit"**, ma è molto più rapida.

> **Suggerimenti**
> La scansione rootkit non è disponibile in Windows XP 64 Bit!

Scansiona registro

Se l'opzione è attivata, viene scansionato il registro alla ricerca di software dannosi.

Processo di scansione

Permetti di arrestare sist. di scansione

Se l'opzione è attivata, la ricerca di virus o programmi indesiderati può essere arrestata in ogni momento con il pulsante "**Arresta"** nella finestra "**Luke Filewalker**". Se questa impostazione è disattivata, il pulsante **Arresta** nella finestra "**Luke Filewalker**" è grigio. Pertanto non è possibile terminare prematuramente una scansione! Questa opzione è attivata di default.

Priorità del sistema di scansione

Il System Scanner differenzia tre livelli di priorità nella scansione diretta. Si tratta di un sistema efficace solo se sul computer sono in esecuzione più processi contemporaneamente. La scelta si ripercuote anche sulla velocità di scansione.

basso

Il System Scanner riceve dal sistema operativo il tempo del processore solo se nessun altro processo necessita di tempo di elaborazione, ovvero finché il System Scanner è l'unico programma in esecuzione, la velocità è massima. Nel complesso, in questo modo viene gestito molto bene anche il lavoro con altri programmi: Il computer è più veloce se altri programmi sono in esecuzione, mentre il System Scanner lavora in background.

medio

Il System Scanner viene eseguito con priorità normale. Tutti i processi ricevono lo stesso tempo di elaborazione dal sistema operativo. Questa opzione è attivata di default ed è consigliata. In alcune circostanze il lavoro con altre applicazioni ne risulta compromesso.

elevato

Il System Scanner riceve la massima priorità. Un lavoro parallelo con altre applicazioni è pressoché impossibile. Tuttavia il System Scanner effettua la scansione in maniera estremamente rapida.

Azione per i rilevamenti

È possibile stabilire delle azioni che System Scanner deve eseguire quando viene rilevato un virus o un programma indesiderato. (Opzioni disponibili solo in Modalità esperto)

Interattivo

Se l'opzione è attivata, i rilevamenti della scansione del System Scanner vengono notificati in una finestra di dialogo. Al termine della scansione, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione di System Scanner.

> **Suggerimenti**
> Di default nella finestra di dialogo è preselezionata l'azione **Quarantena**. È possibile selezionare ulteriori azioni mediante il menu contestuale.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Il System Scanner reagisce conformemente alle impostazioni effettuate precedentemente dall'utente in questa sezione.

Backup in quarantena

Se l'opzione è attivata, il System Scanner crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene mantenuta in quarantena dove il file può essere ripristinato se possiede un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center per ulteriori indagini.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando il System Scanner rileva un virus o un programma indesiderato. Se l'opzione "**Ripara"** è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in "**Azione secondaria"**.

> **Suggerimenti**
> L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

Ripara

Se l'opzione è attivata, il System Scanner ripara automaticamente i file infetti. Se il System Scanner non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

Suggerimenti
Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte del System Scanner.

Rinomina

Se l'opzione è attivata, il System Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

quarantena

Se l'opzione è attivata, il System Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato.Questa procedura è più rapida di **Sovrascrivi ed elimina**(vedere sotto).

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Sovrascrivi ed elimina

Se l'opzione è attivata, il System Scanner sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Azione secondaria

L'opzione "**Azione secondaria"** è selezionabile solo se in "**Azione primaria"** è stata selezionata l'impostazione **Ripara**. Con questa opzione si può decidere cosa fare con il file infetto se non è riparabile.

Rinomina

Se l'opzione è attivata, il System Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

quarantena

Se l'opzione è attivata, il System Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attiva, il file viene eliminato.Questa procedura è più rapida di "Sovrascrivi ed elimina".

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Sovrascrivi ed elimina

Se l'opzione è attivata, il System Scanner sovrascrive il file con un modello standard, infine lo elimina (wipe). Il file non può essere ripristinato.

Suggerimenti
Se si seleziona **Elimina** o **Sovrascrivi ed elimina**come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati, bensì spostati in quarantena.

Archivi

Per la ricerca negli archivi il System Scanner utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. I file compressi vengono scansionati, decompressi e nuovamente scansionati. (Opzioni disponibili solo in Modalità esperto).

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi selezionati nell'elenco degli archivi. Questa opzione è attivata di default.

Tutti i tipi di archivio

Se l'opzione è attivata, vengono selezionati e scansionati i tipi di archivi nella lista di archivi.

Smart Extension

Se l'opzione è attivata, il System Scanner riconosce se un file è in formato compresso (archivio), anche se l'estensione è diversa da quelle abituali, e scansiona l'archivio. Tuttavia a tal fine ogni file deve essere aperto, riducendo così la velocità della scansione. Esempio: se un archivio *.zip ha estensione *.xyz, il System Scanner decomprime anche tale archivio e lo scansiona. Questa opzione è attivata di default.

> **Suggerimenti**
> Vengono scansionati solo quei tipi di archivio che sono selezionati nell'elenco degli archivi.

Limita la profondità di ricorsione

La decompressione e la scansione di archivi particolarmente ramificati può necessitare di molto tempo e molte risorse del sistema. Se l'opzione è attivata, è possibile limitare la profondità della scansione in archivi multipli a un determinato numero di livelli di compressione (profondità di ricorsione massima). In questo modo è possibile risparmiare tempo e risorse del processore.

> **Suggerimenti**
> Per individuare un virus o un programma indesiderato all'interno di un archivio, il System Scanner deve eseguire la scansione fino al livello di ricorsione nel quale si trova il virus o il programma indesiderato.

Profondità massima di ricorsione

Per poter indicare la profondità massima di ricorsione l'opzione **Limita profondità di ricorsione** deve essere attivato.
È possibile inserire direttamente la profondità di ricorsione desiderata oppure modificarla per mezzo dei tasti freccia a destra del campo. I valori consentiti sono compresi tra 1 e 99. Il valore standard e consigliato è 20.

Valori predefiniti

Il pulsante crea i valori predefiniti per la scansione degli archivi.

Elenco archivi

In questa sezione è possibile impostare quali archivi devono essere scansionati dal System Scanner. A tal fine è necessario attivare le voci corrispondenti.

Eccezioni

Oggetti file da escludere dalla scansione (Opzioni disponibili solo in Modalità esperto).

L'elenco in questa finestra contiene file e percorsi che non devono essere presi in considerazione dal System Scanner durante la ricerca di virus e programmi indesiderati.

Si consiglia di inserire quante meno eccezioni possibili e solo i file che non devono essere scansionati durante una scansione normale per qualsivoglia motivo. Consigliamo di far comunque controllare la presenza di virus o programmi indesiderati in questi file prima di inserirli in questo elenco!

Suggerimenti
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Questi file non vengono presi in considerazione durante la scansione!

Suggerimenti
I file inseriti in questa lista vengono segnalati nel file di report. Controllare di tanto in tanto nel file di report la presenza di questi file non scansionati poiché potrebbe non sussistere più il motivo per il quale sono stati esclusi. In questo caso i nomi di questi file dovrebbero essere eliminati dall'elenco.

Campo

Inserire in questo campo il nome del file che non deve essere preso in considerazione durante una scansione diretta. Di default non è indicato alcun file.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se si è fornito un nome di file con un percorso completo, tale file non viene scansionato. Se si è inserito un nome di file senza un percorso, ogni file con tale nome (indipendentemente dal percorso o dal drive) non verrà scansionato.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Suggerimenti
Se si aggiunge un'intera partizione all'elenco dei file da escludere, verranno tralasciati dalla scansione solo i file salvati direttamente nella partizione e non i file contenuti in directory all'interno della partizione:
Esempio: file da omettere: `D:\ = D:\file.txt` viene escluso dalla scansione del System Scanner, `D:\folder\file.txt` viene incluso nella scansione.

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzioni disponibili solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

12.1.2 Report

Il System Scanner possiede una funzione di log molto ampia. In questo modo si ricevono informazioni esatte sui risultati di una scansione diretta. Il file di report contiene tutte le voci del sistema e gli avvisi e i messaggi della scansione diretta. (Opzioni disponibili solo in Modalità esperto.)

> **Suggerimenti**
> Per comprendere quali azioni il System Scanner ha eseguito in caso di rilevamento di virus o programmi indesiderati, deve sempre essere creato un file di report.

Funzione di log

Disabilitato

Se l'opzione è attivata, il System Scanner non riporta le azioni e i risultati della scansione diretta.

Standard

Se l'opzione è attivata, il System Scanner riporta il nome dei file infetti con il percorso. Inoltre, la configurazione per la scansione attuale, le informazioni sulla versione e sul proprietario della licenza viene riportata nel file di report.

Avanzato

Se l'opzione è attivata, il System Scanner riporta anche gli avvisi e le note, oltre alle informazioni standard.

Completo

Se l'opzione è attivata, il System Scanner riporta tutti i file scansionati. Inoltre, tutti i file infetti, nonché gli avvisi e le note vengono registrati nel file di report.

> **Suggerimenti**
> Se l'utente deve inviare un file di report ad Avira (per la ricerca dell'errore), preghiamo di creare il file di report con questa modalità.

12.2 Realtime Protection

La rubrica Realtime Protection della configurazione è dedicata alla configurazione di Realtime Protection. (Opzioni disponibili solo in Modalità esperto).

12.2.1 Cerca

Solitamente si desidera che il proprio sistema sia costantemente monitorato. Per questo viene utilizzato Realtime Protection (scansione in tempo reale = On-Access Scanner). In questo modo è possibile ricercare la presenza di virus e programmi indesiderati in tutti i file che vengono aperti o copiati sul computer "on the fly". (Opzione disponibile solo in Modalità esperto).

File

Realtime Protection può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione.

> **Suggerimenti**
> Se **Tutti i file** è attivo, il pulsante **Estensioni dei file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il programma decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza lista estensione file**, ma molto più sicura poiché i controlli non sono effettuati solamente sulla base delle estensioni dei file.

> **Suggerimenti**
> Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non può essere scelto.

Utilizza la lista delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**. Questa opzione è attivata di default ed è consigliata.

> **Suggerimenti**
> Se questa opzione è attivata e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza elenco estensioni file"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

> **Suggerimenti**
> Prestare attenzione al fatto che l'elenco estensioni dei file può variare da versione a versione.

Modalità di scansione

Qui si stabilisce il momento in cui effettuare la scansione di un file.

Scansione in lettura

Se l'opzione è attivata, Realtime Protection scansiona i file prima che vengano letti o eseguiti da un'applicazione o dal sistema operativo.

Scansione in scrittura

Se l'opzione è attivata, Realtime Protection scansiona un file in scrittura. Dopo questa procedura è possibile accedere nuovamente al file.

Scansione in lettura e scrittura

Se l'opzione è attivata, Realtime Protection scansiona i file prima dell'apertura, della lettura e dell'esecuzione e dopo la scrittura. Questa impostazione è attivata di default e viene consigliata.

Archivi

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Questa opzione è disattivata di default. La scansione degli archivi viene limitata dalla profondità di ricorsione, dal numero di file da scansionare e dalle dimensioni dell'archivio. È possibile impostare la profondità di ricorsione, il numero di file da scansionare e le dimensioni massime dell'archivio.

> **Suggerimenti**
> L'opzione è disattivata di default poiché il processo occupa molta memoria. Generalmente si consiglia di scansionare gli archivi con la scansione diretta.

Profondità massima di ricorsione

Per la ricerca negli archivi, Realtime Protection utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. L'utente può stabilire la profondità di ricorsione. Il valore standard per la profondità di ricorsione è 1 ed è quello consigliato: tutti i file che si trovano direttamente nell'archivio principale vengono scansionati.

Numero max. di file

Per la ricerca negli archivi la scansione viene limitata a un numero massimo di file dell'archivio. Il valore standard per il numero massimo di file da scansionare è 10 e viene consigliato.

Dimensione max. (KB)

Per la ricerca negli archivi la scansione viene limitata a una dimensione degli archivi massima, da decomprimere. Il valore standard è 1000 KB ed è consigliato.

Azione per i rilevamenti

È possibile stabilire delle azioni che Realtime Protection deve eseguire quando viene rilevato un virus o un programma indesiderato. (Opzioni disponibili solo in Modalità esperto).

Interattivo

Se l'opzione è attivata, in caso di rilevamento di un virus da parte di Realtime Protection compare un messaggio sul desktop. È possibile rimuovere il malware rilevato oppure richiamare altre azioni possibili per il trattamento del virus selezionando il pulsante "**Dettagli**". Le azioni vengono visualizzate in una finestra di dialogo. Questa opzione è attivata di default.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Realtime Protection reagisce conformemente alle impostazioni effettuate precedentemente dall'utente in questa sezione.

Backup in quarantena

Se l'opzione è attivata, Realtime Protection crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene conservata in quarantena. Il file può essere ripristinato dal Gestore della quarantena se ha un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center. In base all'oggetto, sono disponibili altre possibilità di scelta nel Gestore della quarantena (vedere Gestore della quarantena).

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Realtime Protection rileva un virus o un programma indesiderato. Se l'opzione "**Ripara**" è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in "**Azione secondaria**".

Suggerimenti
L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

Ripara

Se l'opzione è attivata, Realtime Protection ripara automaticamente i file infetti. Se Realtime Protection non può riparare un file infetto, in alternativa esegue l'opzione selezionata in **Azione secondaria**.

Suggerimenti
Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte di Realtime Protection.

Rinomina

Se l'opzione è attivata, Realtime Protection rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

quarantena

Se l'opzione è attivata, Realtime Protection sposta il file nella directory di quarantena. I file in questa directory possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è più rapida di "Sovrascrivi ed elimina".

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Sovrascrivi ed elimina

Se l'opzione è attivata, Realtime Protection sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Nega accesso

Se l'opzione è attivata, Realtime Protection inserisce il rilevamento solo nel file di report se la funzione di report è attivata. Inoltre, Realtime Protection inserisce una voce nel Log eventi, se questa opzione è attivata.

Attenzione
Quando Realtime Protection è impostato su **Scansione in scrittura**, il file infetto non viene creato.

Azione secondaria

L'opzione "**Azione secondaria"** è disponibile solo se in "**Azione primaria"** è stata selezionata l'opzione**Ripara**. Con questa opzione si può decidere cosa fare con il file infetto se non è riparabile.

Rinomina

Se l'opzione è attivata, Realtime Protection rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

quarantena

Se l'opzione è attivata, Realtime Protection sposta il file nella Quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è più rapida di "Sovrascrivi ed elimina".

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Sovrascrivi ed elimina

Se l'opzione è attivata, Realtime Protection sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Nega accesso

Se l'opzione è attivata, il file infetto non viene creato. Se la funzione di report è stata attivata, Realtime Protection inserisce il rilevamento soltanto nel file di report. Inoltre, Realtime Protection inserisce una voce nel Log eventi, se questa opzione è attivata.

Suggerimenti
Se si seleziona **Elimina** o **Sovrascrivi ed elimina** come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati, bensì spostati in quarantena.

Altre azioni

Utilizza il log degli eventi

Se l'opzione è attivata, viene inserita una voce nel log eventi di Windows a ogni rilevamento. È possibile richiamare gli eventi nel visualizzatore eventi di Windows. Questa opzione è attivata di default. (Opzioni disponibili solo in Modalità esperto).

Eccezioni

Con queste opzioni è possibile configurare gli oggetti soggetti a eccezioni per Realtime Protection (scansione in tempo reale). Gli oggetti identificati verranno così esclusi dalla scansione in tempo reale. Realtime Protection può ignorare gli accessi ai file riportati nell'elenco dei processi da tralasciare durante la scansione in tempo reale. Questa funzione è utile ad esempio per le banche dati o le soluzioni di backup. (Opzioni disponibili solo in Modalità esperto).

Nell'indicare i processi e gli oggetti file da escludere, prestare attenzione a quanto segue: L'elenco viene elaborato dall'alto verso il basso. Più lungo è l'elenco, maggiore è il tempo di cui il processore ha bisogno per elaborare l'elenco a ogni accesso. Si consiglia pertanto di mantenere l'elenco più breve possibile.

Processi esclusi da Realtime Protection

Tutti gli accessi ai file dei processi indicati in questo elenco sono stati esclusi dal monitoraggio mediante Realtime Protection.

Campo

Inserire in questo campo il nome del processo che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun processo.

Il percorso indicato e il nome del file del processo non possono superare i 255 caratteri. È possibile inserire fino a 128 processi. Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Pr indicare i processi è possibile utilizzare caratteri Unicode. Pertanto, è possibile indicare nomi di processi o directory che contengono caratteri speciali.

I drive devono essere indicati nel modo seguente: `[Laufwerksbuchstabe]:\`

Il simbolo dei due punti (:) deve essere utilizzato solo per indicare il drive.

Per indicare il processo, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere):

```
C:\Programme\Anwendung\anwendung.exe
C:\Programme\Anwendung\anwendun?.exe
C:\Programme\Anwendung\anwend*.exe
C:\Programme\Anwendung\*.exe
```

Per evitare che l'intero processo venga escluso dal monitoraggio di Realtime Protection, i dati che contengono esclusivamente i seguenti caratteri non sono validi: *

(asterisco), ? (punto interrogativo), / (barra), \ (barra rovesciata), . (punto), : (due punti).

È possibile escludere dal monitoraggio di Realtime Protection i processi senza percorso completo: `anwendung.exe`

Ciò è valido solo per i processi i cui file eseguibili si trovano sul drive dell'hard disk.

Non indicare alcuna eccezione per i processi i cui file eseguibili si trovano su drive dinamici. I drive dinamici vengono utilizzati per i supporti dati rimovibili, quali CD, DVD o penna USB.

Attenzione
Prestare attenzione al fatto che tutti gli accessi ai file dei processi che sono stati evidenziati nell'elenco sono esclusi dalla scansione di virus e programmi indesiderati! Esplora risorse di Windows e il sistema operativo non possono essere esclusi. La voce corrispondente nell'elenco viene ignorata.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare un file eseguibile.

Processi

Il pulsante "**Processi"** apre la finestra "*Selezione del processo*", in cui vengono indicati i processi in corso.

Aggiungi

Con il pulsante è possibile è possibile accettare il processo indicato nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un processo selezionato dalla finestra di visualizzazione.

Oggetti file da escludere da Realtime Protection

Tutti gli accessi ai file degli oggetti indicati in questo elenco sono esclusi dal monitoraggio mediante Realtime Protection.

Campo

Inserire in questo campo il nome del file che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun file.

Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Per indicare i file da omettere, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere). È possibile anche escludere singole estensioni di file (incluse le wildcard):

```
C:\Verzeichnis\*.mdb
*.mdb
*.md?
*.xls*
C:\Verzeichnis\*.log
```

`V`I nomi delle directory devono concludersi con una barra inversa \, altrimenti viene confuso con un nome di file.

Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.

Per ogni drive è possibile indicare al massimo 20 eccezioni con il percorso completo (che inizia con la lettera del drive).

Es.: `C:\Programme\Anwendung\Name.log`

Il numero massimo di eccezioni senza percorso completo è 64. Es.:

`*.log`

In caso di drive dinamici, collegati (montati) come directory a un altro drive, è necessario utilizzare nell'elenco delle eccezioni il nome dell'alias del sistema operativo per il drive collegato:
ad es. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Anche utilizzando il punto di montaggio stesso (mount point), ad es. `C:\DynDrive`, si esegue comunque la scansione del drive dinamico. È possibile ricavare i nomi dell'alias del sistema operativo da utilizzare dal file di report di Realtime Protection.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare i file da tralasciare.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un file selezionato dalla finestra di visualizzazione.

Per indicare le eccezioni, attenersi alle seguenti indicazioni

Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Un nome di file che contiene wildcard non deve concludersi con una barra inversa.
Ad esempio:
`C:\Programme\Anwendung\anwend*.exe\`
Questa voce non è valida e non viene considerata come un'eccezione!

In base al file di report di Realtime Protection è possibile ricavare i percorsi utilizzati da Realtime Protection durante la ricerca dei file infetti. Nell'elenco delle eccezioni, utilizzare di massima gli stessi percorsi. Procedere come segue: impostare la funzione di log di Realtime Protection nella configurazione in Report su **Completo**. Quindi accedere con Realtime Protection attivato a file, directory, drive collegati. È ora possibile leggere il percorso da utilizzare dal file di report di Realtime Protection. È possibile richiamare il file di report nel Control Center in Realtime Protection.

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzione disponibile solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

12.2.2 ProActiv

ProActiv

L'impiego di Avira ProActiv consente di proteggere il computer da minacce nuove e sconosciute per le quali non esistono ancora definizioni di virus né euristiche. La tecnologia ProActiv è integrata nel componente Realtime Protection e consente di osservare e analizzare le azioni dei programmi. Nel comportamento dei programmi vengono ricercati modelli di azioni tipici dei malware: tipo e svolgimento dell'azione. Se un programma presenta un comportamento tipico di un malware, viene considerato e notificato come un rilevamento di virus : è possibile bloccare l'esecuzione del programma oppure ignorare il messaggio e proseguire. È possibile classificare il programma come affidabile e aggiungerlo così al filtro delle applicazioni dei programmi consentiti. È possibile inoltre aggiungere il programma al filtro delle applicazioni dei programmi da bloccare indicando *Blocca sempre*.

Per rilevare i comportamenti sospetti, il componente ProActiv utilizza set di regole che sono state sviluppate dal Centro Ricerca Malware Avira. Tali set di regole sono alimentati dalle banche dati di Avira.Per la raccolta delle informazioni nelle banche dati Avira, Avira ProActiv invia informazioni relative a programmi sospetti notificati. È possibile disattivare l'inoltro dei dati alle banche dati di Avira.

> **Suggerimenti**
> La tecnologia ProActiv non è ancora disponibile per i sistemi a 64 bit!

Generale (Opzione disponibile solo in Modalità esperto).

Attiva Avira ProActiv

Se l'opzione è attivata, i programmi presenti sul computer vengono monitorati alla ricerca di azioni sospette. Se viene rilevato un comportamento tipico di un malware, si riceve un messaggio. È possibile bloccare il programma oppure proseguire con la sua esecuzione con "**Ignora**". Dal monitoraggio sono esclusi: i programmi classificati come affidabili, i programmi affidabili e firmati che sono contenuti di default nel filtro delle applicazioni consentite, tutti i programmi che sono stati aggiunti dall'utente al filtro delle applicazioni dei programmi consentiti.

Migliorare la sicurezza del proprio computer partecipando alla community Avira ProActiv

Se l'opzione è attivata, Avira ProActiv invia i dati relativi ai programmi sospetti e in alcuni casi file di programma sospetti (file eseguibili) al Centro Ricerca Malware Avira per una verifica avanzata online. Una volta valutati, i dati confluiscono nei set di regole dell'analisi del comportamento ProActiv. In questo modo si prende parte alla

community di Avira ProActiv e si fornisce il proprio contributo al continuo miglioramento e al perfezionamento della tecnologia di sicurezza ProActiv. Se l'opzione è disattivata non vengono inviati dati. Questo non influisce sulla funzionalità di ProActiv.

Per ulteriori informazioni, fare clic qui.

Mediante il link si accede a un sito Internet attraverso il quale si ricevono informazioni dettagliate della verifica avanzata online. I dati completi inviati da una verifica avanzata online sono disponibili sul sito Internet.

Applicazioni da bloccare

In *Applicazioni da bloccare* è possibile inserire applicazioni classificate come dannose e che devono essere bloccate di default da Avira ProActiv. Le applicazioni inserite non possono essere eseguite sul computer. Con l'opzione **Blocca sempre questo programma**, è possibile aggiungere programmi al filtro delle applicazioni da bloccare anche attraverso le comunicazioni di Realtime Protection relative a un comportamento sospetto da parte di un programma.

Applicazioni da bloccare

Applicazione

Nell'elenco sono riportate tutte le applicazioni classificate come dannose e che sono state aggiunte dall'utente durante la configurazione o derivanti dai messaggi del componente ProActiv. Tali applicazioni vengono bloccate da Avira ProActiv e non possono essere eseguite nel sistema. Ogni volta che viene avviato un programma da bloccare, compare un messaggio del sistema operativo. Le applicazioni da bloccare vengono identificate da Avira ProActiv in base al percorso indicato e al nome del file e bloccate indipendentemente dal contenuto.

Campo

Immettere in questo campo l'applicazione da bloccare. Per identificare l'applicazione, è necessario inserire il percorso completo e il nome del file con la relativa estensione. Il percorso indicato deve contenere il drive in cui si trova l'applicazione, oppure iniziare con una variabile d'ambiente.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare l'applicazione da bloccare.

Aggiungi

Con il pulsante "**Aggiungi"** è possibile accettare l'applicazione indicata nel campo nell'elenco delle applicazioni da bloccare.

Suggerimenti
Non è possibile aggiungere le applicazioni necessarie al funzionamento del sistema operativo.

Elimina

Con il pulsante "**Elimina"** è possibile rimuovere un'applicazione selezionata dall'elenco delle applicazioni da bloccare.

Applicazioni da escludere

In *Applicazioni da escludere* sono elencate le applicazioni escluse dal monitoraggio del componente ProActiv: i programmi firmati che sono classificati come affidabili e sono contenuti di default nell'elenco, tutte le applicazioni classificate come affidabili dall'utente e inserite nel filtro delle applicazioni: nella configurazione è possibile aggiungere delle applicazioni all'elenco delle applicazioni consentite. È inoltre possibile aggiungere delle applicazioni segnalate nelle comunicazioni di Realtime Protection relative a un comportamento sospetto da parte di un programma, attivando l'opzione nei messaggi di Realtime Protection **Programma attendibile**.

Applicazioni da escludere

Applicazione

L'elenco contiene le applicazioni escluse dal monitoraggio del componente ProActiv. Nelle impostazioni di default dopo l'installazione, l'elenco contiene applicazioni firmate di produttori attendibili. È possibile inserire applicazioni classificate come attendibili mediante la configurazione o i messaggi di Realtime Protection. Il componente ProActiv identifica le applicazioni in base al percorso, al nome del file e al contenuto. La verifica dei contenuti è utile poiché a un programma possono essere aggiunti codici dannosi in un secondo momento, in seguito a modifiche come gli aggiornamenti. Specificando la **modalità**, è possibile stabilire se deve essere eseguita una verifica del contenuto: Con la modalità "*Contenuto"*, vengono verificate le modifiche del contenuto nei file delle applicazioni indicate con percorso e nome prima che vengano escluse dal monitoraggio mediante il componente ProActiv. Nel caso di una modifica del contenuto del file, l'applicazione viene nuovamente monitorata dal componente ProActiv. Con la modalità "*Percorso"* non avviene alcuna verifica del contenuto prima che l'applicazione venga esclusa dal monitoraggio mediante Realtime Protection. Per cambiare la modalità di esclusione, fare clic sulla modalità indicata.

Attenzione
Utilizzare la modalità *Percorso* solo in casi eccezionali. In seguito a un aggiornamento, è possibile che a un'applicazione vengano aggiunti codici dannosi. L'applicazione che originariamente era innocua, ora è un malware.

> **Suggerimenti**
> Alcune applicazioni affidabili, ad esempio tutti i componenti applicativi del prodotto Avira, sono esclusi di default dal monitoraggio mediante ProActiv, tuttavia non sono riportati nell'elenco.

Campo

Inserire in questo campo l'applicazione che si intende escludere dal monitoraggio mediante il componente ProActiv. Per identificare l'applicazione, è necessario inserire il percorso completo e il nome del file con la relativa estensione. Il percorso indicato deve contenere il drive in cui si trova l'applicazione, oppure iniziare con una variabile d'ambiente.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare l'applicazione da escludere.

Aggiungi

Con il pulsante "**Aggiungi"**, è possibile accettare l'applicazione indicata nel campo nell'elenco delle applicazioni da escludere.

Elimina

Con il pulsante "**Elimina"**, è possibile rimuovere un'applicazione selezionata dall'elenco delle applicazioni da escludere.

12.2.3 Report

Realtime Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento. " ?> (Opzione disponibile solo in Modalità esperto).

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Realtime Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Realtime Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, Realtime Protection registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Realtime Protection registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata il file del report viene salvato prima dell'abbreviazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

12.3 Aggiornamento

Nella rubrica **Aggiornamento** configurare l'esecuzione automatica degli aggiornamenti. È possibile impostare diversi intervalli di aggiornamento.

Aggiornamento automatico

ogni n giorno/i / ora/e / minuto/i

In questo campo è possibile indicare l'intervallo in cui devono essere eseguiti gli aggiornamenti automatici. Per modificare l'intervallo di aggiornamento, è possibile indicare un dato temporale nel campo e modificarlo mediante i tasti freccia a destra del campo.

Avvia il job all'avvio della connessione Internet (dial-up)

Se l'opzione è attivata, oltre all'intervallo di aggiornamento stabilito, il job di aggiornamento viene eseguito quando si attiva una connessione a Internet. (Opzione disponibile solo in Modalità esperto).

Ripeti job se il tempo è scaduto

Se l'opzione è attivata, vengono eseguiti job di aggiornamento scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento. (Opzione disponibile solo in Modalità esperto).

12.3.1 Aggiornamento di prodotto

In **Aggiornamento prodotto** configurare l'esecuzione degli aggiornamenti del prodotto o la notifica della disponibilità di tali aggiornamenti. (Opzioni disponibili solo in Modalità esperto).

Aggiornamenti prodotto

Scarica aggiornamenti del prodotto e installa automaticamente

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati e installati automaticamente, non appena si rendono disponibili, dai componenti di aggiornamento. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Scaricare aggiornamenti del prodotto. Se è necessario riavviare, installare l'aggiornamento dopo il successivo riavvio del sistema, altrimenti eseguire immediatamente l'installazione.

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati non appena disponibili. L'aggiornamento viene installato automaticamente dopo il download dei file di aggiornamento, qualora non sia necessario il riavvio. Se si tratta di un aggiornamento del prodotto che richiede il riavvio del computer, tale aggiornamento non viene eseguito subito dopo il download dei file di aggiornamento, bensì solo dopo il successivo riavvio del sistema effettuato dall'utente. Il vantaggio che ne deriva è che il riavvio non viene eseguito mentre l'utente sta lavorando al computer. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Avvisa quando sono disponibili nuovi aggiornamenti del prodotto

Se l'opzione è attivata, si viene avvisati solo se sono disponibili nuovi aggiornamenti per il prodotto. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e

collegamento esistente a un server di download.La notifica avviene tramite un messaggio sul desktop sotto forma di una finestra di pop up e tramite un avviso dell'Updater nel Control Center in Panoramica > Eventi.

Avvisa nuovamente dopo n giorno(i)

Indicare in questo campo dopo quanti giorni si desidera ricevere nuovamente la notifica relativa alla disponibilità degli aggiornamenti del prodotto, qualora l'aggiornamento del prodotto non sia stato eseguito alla prima notifica.

Non scaricare aggiornamenti prodotto

Se l'opzione è attivata, non si effettuano aggiornamenti automatici o notifiche se sono disponibili aggiornamenti del prodotto mediante l'Updater. Gli aggiornamenti del file delle definizioni dei virus e del motore di ricerca avvengono sempre indipendentemente da questa impostazione.

Attenzione
L'aggiornamento del file di definizione dei virus e del motore di ricerca avviene contestualmente a ogni aggiornamento effettuato, indipendentemente dalle impostazioni per l'aggiornamento di prodotto (vedere Aggiornamenti).

Suggerimenti
Se è stata attivata l'opzione per l'aggiornamento automatico del prodotto, è possibile configurare ulteriori opzioni di notifica e possibilità di interruzione del riavvio in Impostazioni riavvio. (Opzioni disponibili solo in Modalità esperto).

12.3.2 Riavvio impostazioni

Quando viene eseguito un aggiornamento del prodotto Avira, può essere necessario un riavvio del sistema. Se è stata impostata un'esecuzione automatica dell'aggiornamento del prodotto in Aggiornamento > Aggiornamento prodotto, è possibile scegliere fra diverse opzioni di notifica e per l'interruzione del riavvio in **Impostazioni riavvio**. (Opzioni disponibili solo in Modalità esperto).

Suggerimenti
Nell'effettuare le impostazioni di riavvio, si noti che nella configurazione è possibile scegliere fra due opzioni per l'esecuzione degli aggiornamenti del prodotto con riavvio necessario del computer, in Aggiornamento > Aggiornamento prodotto:
- **Scarica aggiornamenti del prodotto e installa automaticamente**: L'aggiornamento e il riavvio vengono eseguiti quando l'utente sta utilizzando il computer. Se è stata attivata questa opzione, possono essere utili le routine di riavvio con possibilità di interruzione oppure con funzione di avviso.
- **Scaricare aggiornamenti del prodotto. Se è necessario riavviare,**

installare l'aggiornamento dopo il successivo riavvio del sistema, altrimenti eseguire immediatamente l'installazione: l'aggiornamento e il riavvio vengono eseguiti dopo che l'utente ha avviato il computer e si è registrato. Per questa opzione sono consigliabili le routine di riavvio automatiche.

Riavvio del sistema dopo n secondi (con conto alla rovescia, nessuna possibilità di interruzione)

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo l'esecuzione di un aggiornamento del prodotto secondo l'intervallo di tempo indicato. Compare un conto alla rovescia, senza possibilità di interrompere il riavvio del sistema.

Ricordo periodico di riavvio

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Nell'intervallo di tempo indicato, vengono visualizzati avvisi di riavvio senza possibilità di interruzione. Negli avvisi è possibile confermare il riavvio del sistema oppure selezionare l'opzione "**Ricorda ancora"**.

Richiesta di esecuzione di riavvio del sistema

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Viene visualizzato una sola volta un messaggio in cui è possibile confermare il riavvio oppure interrompere la routine di riavvio.

Riavvio del sistema senza richiesta

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo un aggiornamento del prodotto. Non si riceve alcun messaggio.

12.3.3 Server web

Server web

L'aggiornamento può essere eseguito direttamente mediante server web in Internet. (Opzioni disponibili solo in Modalità esperto).

Connessione al server Web

Utilizza una connessione esistente (rete)

Questa impostazione viene visualizzata se viene utilizzata la connessione mediante una rete.

Utilizzare la seguente connessione:

Questa impostazione viene visualizzata se si definisce individualmente la connessione.

L'Updater riconosce automaticamente quali opzioni di connessione sono disponibili. Le opzioni di connessione non disponibili sono grigie e non possono essere attivate. Ad esempio, è possibile creare manualmente una connessione dial-up mediante una voce dell'elenco telefonico di Windows.

Utente

inserire il nome utente dell'account selezionato.

Password

inserire la password per questo account. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

Suggerimenti
Se sono stati dimenticati il nome utente o la password di un account Internet contattare il provider di servizi Internet.

Suggerimenti
La selezione automatica dell'Updater mediante i cosiddetti strumenti dial-up (ad esempio SmartSurfer, Oleco, ...) attualmente non è ancora disponibile.

Termina la connessione dial-up al termine dell'aggiornamento

Se l'opzione è attivata, viene interrotta automaticamente la connessione dial-up aperta per l'aggiornamento, non appena il download è stato eseguito con successo.

Suggerimenti
L'opzione non è disponibile in Vista e in Windows 7. In Vista e in Windows 7 la connessione dial-up, aperta per l'aggiornamento, viene sempre interrotta, non appena il download è stato eseguito.

Impostazioni proxy

Proxyserver

Non utilizzare un server Proxy

Se l'opzione è attivata, la connessione al server web viene effettuata mediante un server proxy.

Utilizza impostazioni di sistema di Windows

Se l'opzione è attivata, vengono utilizzate le impostazioni di sistema di Windows correnti per la connessione al server Web mediante un server proxy. Per configurare le impostazioni di sistema di Windows per l'utilizzo di un server proxy, accedere a **Pannello di controllo > Opzioni Internet > Connessioni > Impostazioni LAN**. È possibile accedere alle opzioni Internet anche nel menu **Extra** di Internet Explorer.

> **Attenzione**
> Quando si utilizza un server proxy che richiede l'autenticazione, immettere tutti i dati tramite l'opzione **Utilizza questo server proxy**. Per i server proxy senza autenticazione, è possibile utilizzare l'opzione **Utilizza impostazioni di sistema di Windows**.

Utilizza questo server proxy

Se l'opzione è attivata, la connessione al server web avviene mediante un server proxy, utilizzando le impostazioni definite.

Indirizzo

Immettere il nome computer o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Porta

Immettere il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Nome Login

Immettere un nome utente per la registrazione sul server proxy.

Password

Inserire la password appropriata per la registrazione sul server proxy. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

Esempi:

Indirizzo: `proxy.domain.de` Porta: `8080`

Indirizzo: `192.168.1.100` Porta: `3128`

12.4 Backup

In **Configurazione > Sicurezza Internet > Backup** è possibile configurare il componente Backup. (Opzioni disponibili solo in Modalità esperto).

12.4.1 Impostazione

In **Impostazioni** è possibile configurare il comportamento del componente Backup.

Esegui backup solo file modificati

Se l'opzione è attivata viene creato un backup incrementale: vengono memorizzati nel profilo di backup solo i file che sono stati modificati dopo l'ultimo backup. Se l'opzione è disattivata, ogni volta che si memorizza un profilo di backup viene eseguito un backup completo: tutti i file nel profilo di backup vengono memorizzati. L'opzione è

normalmente attivata e consigliata poiché i backup incrementali sono più rapidi e consumano meno risorse dei backup di tutti i dati.

Verifica malware prima del backup

Se l'opzione è attivata, i file da memorizzare vengono controllati per verificare la presenza di virus e malware al momento del backup. I file infetti non vengono salvati. Questa opzione normalmente è attivata e consigliata.

12.4.2 Eccezioni

In **Eccezioni** è possibile definire quali oggetti file e tipi di file inserire o meno nel backup.

Oggetti file da escludere dal backup

L'elenco in questa finestra contiene file e percorsi che non devono essere memorizzati in un backup.

> **Suggerimenti**
> Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

> **Suggerimenti**
> I file inseriti in questa lista vengono segnalati nel file di report.

Campo

In questo campo è necessario immettere i nomi degli oggetti file che non si desidera memorizzare. Normalmente viene indicato il percorso di una directory temporanea per le impostazioni locali dell'utente registrato.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se è stato immesso un nome file con il percorso completo, tale file non verrà memorizzato. Se è stato immesso un nome file senza percorso, tutti i file con quel nome (indipendentemente dal percorso e dal drive) non vengono memorizzati.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Resetta lista

Questo pulsante ripristina i valori standard predefiniti.

Prestare attenzione ai seguenti punti

- Le wildcard * (numero di caratteri desiderato) e ? (un solo carattere) sono consentite solo nei nomi del file.
- L'elenco viene elaborato dall'alto verso il basso.
- Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.
- È possibile anche escludere singole estensioni di file (incluse le wildcard).
- Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

> **Suggerimenti**
> Un nome di file che contiene wildcard non deve concludersi con una barra inversa. Ad esempio:
> `C:\Programmi\Applicazioni\applicaz*.exe\`
> Questa voce non è valida e non viene considerata come un'eccezione!

Esempi

- `anwendung.exe`
- `\Programme\`
- `C:\*.*`
- `C:\*`
- `*.exe`
- `*.xl?`
- `*.*`
- `C:\Programme\Anwendung\anwendung.exe`
- `C:\Programme\Anwendung\anwend*.exe`
- `C:\Programme\Anwendung\anwend*`
- `C:\Programme\Anwendung\anwend????.e*`
- `C:\Programme\`
- `C:\Programme`
- `C:\Programme\Anwendung\*.mdb`

Liste estensioni file

Considerare tutte le estensioni dei file

Se l'opzione è attivata tutti i file nel profilo di backup vengono memorizzati.

Attiva elenco delle estensioni file da tralasciare

Se l'opzione è attivata vengono salvati tutti i file nel profilo di backup, tranne quelli con estensione corrispondente alle estensioni riportate nell'elenco delle estensioni dei file da escludere.

Estensioni file

Questo pulsante consente di richiamare una finestra di dialogo in cui vengono visualizzate tutte le estensioni dei file che non vengono memorizzati in un backup se l'opzione "**Attiva elenco delle estensioni file da tralasciare**" è attivata. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Attiva elenco delle estensioni file da considerare

Se l'opzione è attivata vengono memorizzati solo i file con estensione compresa nell'elenco delle estensioni dei file da considerare.

Estensioni file

Questo pulsante consente di richiamare una finestra di dialogo in cui vengono visualizzate tutte le estensioni dei file che vengono memorizzati in un backup se l'opzione "**Attiva elenco delle estensioni file da considerare**" è attivata. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

12.4.3 Report

Il componente Backup offre una vasta funzione di log.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, il componente Backup non crea alcun log. Rinunciare al log solo in casi eccezionali.

Standard

Se l'opzione è attivata, il componente Backup raccoglie informazioni importanti (per la memorizzazione, per i rilevamenti dei virus, per avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, il componente Backup registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, il componente Backup registra tutte le informazioni sul backup e sulla scansione per i virus nel file di report.

12.5 FireWall

La rubrica **FireWall** in **Sicurezza Internet > Configurazione** è dedicata alla configurazione del FireWall Avira.

12.5.1 Regole adattatore

Il FireWall di Avira considera adattatore qualsivoglia unità hardware simulata da un software (ad esempio Miniport, Bridge Connection, ecc.) o qualsivoglia unità hardware (ad esempio una scheda di rete).

Il FireWall di Avira visualizza le regole adattatore per tutti gli adattatori presenti sul computer per i quali è installato un driver. (Opzioni disponibili solo in Modalità esperto).

- Protocollo ICMP
- TCP Port-Scan
- UDP Port-Scan
- Regola in entrata
- Regola protocollo IP in entrata
- Regola in uscita
- Pulsanti

Una regola adattatore predefinita dipende dal livello di sicurezza. È possibile variare il *livello di sicurezza* tramite la rubrica Sicurezza Internet > FireWall del Control Center o adattare le regole adattatore alle proprie esigenze. Se le regole adattatore sono state adeguate alle proprie esigenze, nella rubrica FireWall del Control Center, nella sezione *Livello di sicurezza*, il cursore sarà posizionato su **Utente**.

> **Suggerimenti**
> L'impostazione standard del livello di sicurezza per tutte le regole predefinite del Firewall di Avira è **medio**.

Protocollo ICMP

L'Internet Control Message Protocol (ICMP) serve allo scambio di informazioni o comunicazione di errori nelle reti. Il protocollo viene utilizzato anche per le comunicazioni sullo status per mezzo di Ping o Tracert.
Con questa regola è possibile definire le tipologie ICMP in entrata e in uscita che dovrebbero essere bloccate, fissare i parametri per il flooding e definire il comportamento

da tenere in caso di pacchetti ICMP frammentati. Questa regola serve a evitare i cosiddetti attacchi ICPM Flood, che potrebbero comportare un carico o un sovraccarico del processore del computer attaccato, poiché risponde a ogni pacchetto.

Regole predefinite per il protocollo ICMP

Impostazione	Regole
Basso	Tipi in entrata bloccati: **nessun tipo**. Tipi in uscita bloccati: **nessun tipo**. Supporre un flooding se il ritardo tra i pacchetti è inferiore a **50** millisecondi. **Rifiuta** pacchetti ICMP frammentati.
Medio	La stessa regola applicata con l'impostazione livello basso.
Elevato	Tipi in entrata bloccati: **diversi tipi**. Tipi in uscita bloccati: **diversi tipi**. Supporre un flooding se il ritardo tra i pacchetti è inferiore a **50** millisecondi. **Rifiuta** pacchetti ICMP frammentati.

Tipi in entrata bloccati: nessun tipo/diversi tipi

Facendo clic sul link si apre un elenco contenente i tipi di pacchetti ICMP. Da questi elenchi è possibile selezionare i tipi ICMP che si desidera bloccare.

Tipi in uscita bloccati: nessun tipo/diversi tipi

Facendo clic sul link si apre un elenco contenente i tipi di pacchetti ICMP. Dall'elenco è possibile selezionare le tipologie di notifiche ICMP che si desidera bloccare.

Supporre un flooding

Facendo clic sul link si apre una finestra di dialogo in cui è possibile inserire il valore massimo per il ritardo ICMP consentito.

Pacchetti ICMP frammentati

Facendo clic sul link si ha la possibilità di scegliere se "**accettare**" o "**non accettare**" i pacchetti ICMP frammentati.

Port-Scan TCP

Con questa regola è possibile definire quando il FireWall deve supporre un Port-Scan TCP e come comportarsi in un caso del genere. Questa regola serve a evitare i cosiddetti attacchi Port-Scan TCP mediante i quali si creano porte aperte sul computer. Gli attacchi di questo tipo vengono principalmente usati per sfruttare i punti deboli del proprio computer che serviranno poi per eseguire attacchi pericolosi.

Regole predefinite per il Port-Scan TCP

Impostazione	Regole
Basso	Supporre un Port-Scan TCP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan TCP, scrivere nella **banca dati degli eventi** l'indirizzo IP dell'aggressore e **non aggiungerlo** alle regole per bloccare l'attacco.
Medio	Supporre un Port-Scan TCP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan TCP, scrivere nella **banca dati degli eventi** l'indirizzo IP dell'aggressore e **aggiungerlo** alle regole per bloccare l'attacco.
Elevato	La stessa regola applicata con l'impostazione livello medio.

Porte

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile immettere il numero di porte che devono essere scansionate, in modo da escludere un Port-Scan TCP.

Finestra temporale del Port-Scan

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile immettere l'intervallo di tempo in cui un determinato numero di porte dovrebbe essere scansionato, in modo da escludere un Port-Scan TCP.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere se scrivere o meno l'indirizzo IP dell'aggressore nella banca dati degli eventi.

Regola

Facendo clic sul link si ha la possibilità di decidere se aggiungere o meno la regola per il blocco dell'attacco Port-Scan TCP.

Port-Scan UDP

Con questa regola è possibile definire quando il FireWall deve supporre un Port-Scan UDP e come comportarsi in un caso del genere. Questa regola serve a evitare i cosiddetti attacchi Port-Scan UDP mediante i quali si creano porte aperte sul proprio computer. Gli attacchi di questo tipo vengono principalmente usati per sfruttare i punti deboli del proprio computer che serviranno poi per eseguire attacchi pericolosi.

Regole predefinite per il Port-Scan UDP

Impostazione	Regole
Basso	Supporre un Port-Scan UDP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan UDP, scrivere nella **banca dati degli eventi** l'indirizzo IP dell'aggressore e **non aggiungerlo** alle regole per bloccare l'attacco.
Medio	Supporre un Port-Scan UDP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan TCP, scrivere nella **banca dati degli eventi** l'indirizzo IP dell'aggressore e **aggiungerlo** alle regole per bloccare l'attacco.
Elevato	La stessa regola applicata con l'impostazione livello medio.

Porte

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile immettere il numero di porte che devono essere scansionate, in modo da escludere un Port-Scan UDP.

Finestra temporale del Port-Scan

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile immettere l'intervallo di tempo in cui un determinato numero di porte dovrebbe essere scansionato, in modo da escludere un Port-Scan UDP.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere se scrivere o meno l'indirizzo IP dell'aggressore nella banca dati degli eventi.

Regola

Facendo clic sul link si ha la possibilità di decidere se aggiungere o meno la regola per il blocco dell'attacco Port-Scan UDP.

Regole in entrata

Le regole in entrata servono a controllare lo scambio dati in entrata con il Firewall di Avira.

> **Attenzione**
> Dal momento che per filtrare un pacchetto vengono applicate le regole una dopo l'altra, la loro sequenza è di particolare importanza. Si prega di modificare la sequenza delle regole solo quando si è completamente sicuri del risultato che si otterrà.

Regole predefinite per il monitoraggio dello scambio dati TCP

<table>
<tr><th>Impostazione</th><th>Regole</th></tr>
<tr><td>Basso</td><td>Lo scambio di dati in entrata non viene bloccato dal FireWall di Avira.</td></tr>
<tr><td>Medio</td><td>
Consenti la connessione TCP esistente sulla porta 135
Consenti pacchetti TCP, dall'indirizzo 0.0.0.0 con maschera 0.0.0.0, se la porta locale è {135} e la porta remota {0-65535}.
Applica ai pacchetti delle connessioni disponibili.
Non scrivere nella banca dati degli eventi se il pacchetto corrisponde alla regola.
Esteso: seleziona i pacchetti con i seguenti byte con maschera all’offset 0.
Rifiuta pacchetti TCP sulla porta 135
Rifiuta pacchetti TCP, dall'indirizzo 0.0.0.0 con maschera 0.0.0.0, se la porta locale è {135} e la porta remota {0-65535}.
Applica a tutti i pacchetti.
Non scrivere nella banca dati degli eventi se il pacchetto corrisponde alla regola.
Esteso: seleziona i pacchetti con i seguenti byte con maschera all’offset 0.
Monitoraggio del traffico dati conforme TCP
Consenti pacchetti TCP, dall'indirizzo 0.0.0.0 con maschera 0.0.0.0, se la porta locale è {0-65535} e la porta remota {0-65535}.
Applica all'inizio della creazione di una connessione e ai pacchetti delle connessioni disponibili.
Non scrivere nella banca dati degli eventi se il pacchetto corrisponde alla regola.
Avanzato: seleziona i pacchetti con i seguenti byte con maschera all’offset 0.
Rifiuta tutti i pacchetti TCP
Rifiuta pacchetti TCP, dall'indirizzo 0.0.0.0 con maschera 0.0.0.0, se la porta locale è {0-65535} e la porta remota {0-65535}.
Applica a tutti i pacchetti.
Non scrivere nella banca dati degli eventi se il pacchetto corrisponde alla regola.
Avanzato: seleziona i pacchetti con i seguenti byte con maschera all’offset 0.
</td></tr>
</table>

Elevato	**Monitorare il traffico dati TCP consentito** **Consenti** pacchetti TCP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{0-65535}**. Applica ai **pacchetti delle connessioni disponibili**. **Non scrivere nella banca dati degli eventi** se il pacchetto corrisponde alla regola. Avanzato: seleziona i pacchetti con i seguenti byte con maschera all'offset **0**.

Consenti/rifiuta pacchetti TCP

Facendo clic sul link si ha la possibilità di decidere se consentire o rifiutare i pacchetti TCP speciali definiti.

Indirizzo IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IPv4 o IPv6 desiderati.

Maschera IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire la maschera IPv4 o IPv6 desiderata.

Porte locali

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire una o più porte locali e anche intere sezioni delle porte.

Porte remote

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire una o più porte remote e anche intere sezioni delle porte.

Metodi di applicazione

Facendo clic sul link si ha la possibilità di utilizzare la regola sui pacchetti di connessioni disponibili all'inizio della creazione della connessione e i pacchetti delle connessioni esistenti o su tutte le connessioni.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere di scrivere o meno nella banca dati degli eventi se il pacchetto corrisponde alla regola.

Avanzato

L'opzione **Esteso** consente una filtrazione a causa del contenuto. È possibile così, ad esempio, rifiutare i pacchetti che contengono dati specifici con un offset preciso. Se non si desidera utilizzare questa opzione non selezionare alcun file o selezionare un file vuoto.

Filtrazione per contenuto: byte

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare il file che contiene il buffer speciale.

Filtrazione per contenuto: maschera

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare la maschera speciale.

Filtrazione per contenuto: offset

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire l'offset per la filtrazione di contenuti. L'offset viene calcolato dalla fine dell'header TCP.

Regole predefinite per il monitoraggio dello scambio dati UDP

Impostazione	Regole
Basso	-
Medio	• **Monitoraggio del traffico dati conforme UDP** **Consenti** pacchetti UDP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{0-65535}**. Applica la regola alle **porte aperte** per **tutti i flussi di dati**. **Non scrivere nella banca dati degli eventi** se il pacchetto corrisponde alla regola. Avanzato: seleziona i pacchetti con i seguenti byte con maschera all'offset **0**. • **Rifiuta tutti i pacchetti UDP** **Rifiuta** pacchetti UDP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{0-65535}**. Applica a **tutte le porte** per **tutti i flussi di dati**. **Non scrivere nella banca dati degli eventi** se il pacchetto corrisponde alla regola. Avanzato: seleziona i pacchetti con i seguenti byte con maschera all'offset **0**.

Elevato	**Monitorare il traffico dati UDP consentito** **Consenti** pacchetti UDP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{53, 67, 68, 88,...}**. Applica la regola alle **porte aperte** per **tutti i flussi di dati**. **Non scrivere nella banca dati degli eventi** se il pacchetto corrisponde alla regola. Avanzato: seleziona i pacchetti con i seguenti byte con maschera all’offset **0**.

Consenti/rifiuta pacchetti UDP

Facendo clic sul link si ha la possibilità di decidere se consentire o rifiutare i pacchetti UDP speciali definiti.

Indirizzo IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IPv4 o IPv6 desiderati.

Maschera IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire la maschera IPv4 o IPv6 desiderata.

Porte locali

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire una o più porte locali e anche intere sezioni delle porte.

Porte remote

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire una o più porte remote e anche intere sezioni delle porte.

Metodi di applicazione

Porte

Facendo clic sul link si ha la possibilità di decidere se si desidera applicare la regola a tutte le porte o solo alle porte aperte.

Flussi di dati

Facendo clic sul link si ha la possibilità di decidere se si desidera applicare la regola a tutti i flussi di dati o solo ai flussi di dati in uscita.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere di scrivere o meno nella banca dati degli eventi se il pacchetto corrisponde alla regola.

Avanzato

L'opzione **Esteso** consente una filtrazione a causa del contenuto. È possibile così, ad esempio, rifiutare i pacchetti che contengono dati specifici con un offset preciso. Se non si desidera utilizzare questa opzione non selezionare alcun file o selezionare un file vuoto.

Filtrazione per contenuto: byte

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare il file che contiene il buffer speciale.

Filtrazione per contenuto: maschera

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare la maschera speciale.

Filtrazione per contenuto: offset

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire l'offset per la filtrazione di contenuti. L'offset viene calcolato dalla fine dell'header UDP.

Regole predefinite per il monitoraggio dello scambio dati ICMP

Impostazione	Regole
Basso	-
Medio	**Non rifiutare pacchetti ICMP sulla base dell'indirizzo IP** **Consenti** pacchetti ICMP dell'indirizzo **0.0.0.0** con maschera **0.0.0.0**. **Non scrivere nella banca dati degli eventi** se il pacchetto corrisponde alla regola. Avanzato: seleziona i pacchetti con i seguenti byte con maschera all'offset **0**.
Elevato	La stessa regola applicata con l'impostazione livello medio.

Consenti/rifiuta pacchetti ICMP

Facendo clic sul link si ha la possibilità di decidere se consentire o rifiutare i pacchetti ICMP speciali definiti.

Indirizzo IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IPv4 desiderati.

Maschera IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire la maschera IPv4 desiderata.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere di scrivere o meno in una banca dati degli eventi se il pacchetto corrisponde alla regola.

Avanzato

L'opzione **Esteso** consente una filtrazione a causa del contenuto. È possibile così, ad esempio, rifiutare i pacchetti che contengono dati specifici con un offset preciso. Se non si desidera utilizzare questa opzione non selezionare alcun file o selezionare un file vuoto.

Filtrazione per contenuto: byte

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare il file che contiene il buffer speciale.

Filtrazione per contenuto: maschera

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare la maschera speciale.

Filtrazione per contenuto: offset

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire l'offset per la filtrazione di contenuti. L'offset viene calcolato dalla fine dell'header ICMP.

Regola predefinita per i pacchetti IP

Impostazione	Regole
Basso	-
Medio	-
Elevato	**Rifiuta tutti i pacchetti IP** **Rifiuta** pacchetti **IPv4** dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**. **Non scrivere nella banca dati degli eventi** se il pacchetto corrisponde alla regola.

Consenti/rifiuta

Facendo clic sul link si ha la possibilità di decidere se consentire o rifiutare i pacchetti IP speciali definiti.

IPv4 / IPv6

Facendo clic sul link è possibile scegliere tra IPv4 e IPv6.

Indirizzo IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IPv4 o IPv6 desiderati.

Maschera IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire la maschera IPv4 o IPv6 desiderata.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere di scrivere o meno nella banca dati degli eventi se il pacchetto corrisponde alla regola.

Regola protocollo IP in entrata

Accettazione / rifiuto

Facendo clic sul link si ha la possibilità di decidere se consentire o rifiutare i pacchetti IP speciali definiti.

Indirizzo IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IPv4 o IPv6 desiderati.

Maschera IP

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile inserire la maschera IPv4 o IPv6 desiderata.

Protocollo

Facendo clic sul link si apre una finestra di dialogo nella quale è possibile selezionare il protocollo IP desiderato.

Banca dati degli eventi

Facendo clic sul link si ha la possibilità di decidere di scrivere o meno nella banca dati degli eventi se il pacchetto corrisponde alla regola.

Regole in uscita

Le regole in uscita servono a controllare lo scambio dati in uscita con il FireWall di Avira. È possibile definire una regola in uscita per i seguenti protocolli: IP, ICMP, UDP e TCP.

Attenzione
Dal momento che per filtrare un pacchetto vengono applicate le regole una dopo l'altra, la loro sequenza è di particolare importanza. Si prega di modificare la sequenza delle regole solo quando si è completamente sicuri del risultato che si otterrà.

Pulsanti

Pulsanti	Descrizione
Aggiungi	Consente la creazione di una nuova regola. Facendo clic su questo pulsante appare la finestra di dialogo "Aggiungi nuova regola". In questa finestra di dialogo è possibile selezionare nuove regole.
Cancella	Elimina una regola selezionata.
In alto	Spostare una regola selezionata in una posizione verso l'alto aumentando in tal modo la priorità di questa regola.
In basso	Spostare una regola selezionata in una posizione verso il basso riducendo in tal modo la priorità di questa regola.
Rinomina	Rinomina una regola selezionata.

Suggerimenti
È possibile aggiungere nuove regole per i singoli adattatori o anche per tutti gli adattatori disponibili del computer. Per aggiungere una regola adattatore per tutti gli adattatori, selezionare **Risorse del computer** nella struttura dell'adattatore visualizzata e fare clic sul pulsante **Aggiungi**. Vedere Aggiungi nuova regola.

Suggerimenti
Per modificare la posizione di una regola, è possibile anche trascinare la regola nella posizione desiderata utilizzando il mouse.

12.5.2 Aggiungere nuova regola

In questa finestra si possono selezionare nuove regole in entrata e in uscita. La regola selezionata viene inserita con attributi standard nella finestra **Regole adattatore** dove può essere ulteriormente personalizzata. Oltre alle regole in entrata e in uscita, sono disponibili altre regole.

Possibili regole

Consenti rete peer-to-peer

Consente le connessioni peer-to-peer: comunicazione TCP in ingresso sulla Porta 4662 e comunicazione UDP in ingresso sulla Porta 4672

Porta TCP

Facendo clic con il mouse sul link, si apre una finestra di dialogo nella quale è possibile immettere la porta TCP consentita.

Porta UDP

Facendo clic con il mouse sul link, si apre una finestra di dialogo nella quale è possibile immettere la porta UDP consentita.

Consenti collegamenti VMWARE

Consente la comunicazione fra sistemi VMWare

Blocca indirizzi IP

Blocca l'intero traffico di un indirizzo IP specifico

Versione IP

Facendo clic sul link è possibile scegliere tra IPv4 e IPv6.

Indirizzo IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IPv4 o IPv6 desiderato.

Blocca subnet

Blocca l'intero traffico da un indirizzo IP e da una maschera di sottorete specifici

Versione IP

Facendo clic sul link è possibile scegliere tra IPv4 e IPv6.

Indirizzo IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP desiderato.

Maschera di sottorete

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la maschera di sottorete desiderata.

Consenti indirizzi IP

Consente l'intero traffico da un indirizzo IP specifico

Versione IP

Facendo clic sul link è possibile scegliere tra IPv4 e IPv6.

Indirizzo IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP desiderato.

Consenti subnet

Consente l'intero traffico da un indirizzo IP e una maschera di sottorete specifici

Versione IP

Facendo clic sul link è possibile scegliere tra IPv4 e IPv6.

Indirizzi IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP desiderato.

Maschera di sottorete

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la maschera di sottorete desiderata.

Consenti server Web

Consente la comunicazione da un server Web sulla Porta 80: comunicazione TCP in ingresso sulla Porta 80

Porta

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la porta utilizzata dal server web.

Consenti connessioni VPN

Consente connessioni VPN (Virtual Private Network) con un indirizzo IP definito: traffico dati UDP in ingresso su x Porte, traffico dati TCP in ingresso su x Porte, traffico dati IP in ingresso con protocolli ESP(50), GRE (47)

Versione IP

Facendo clic sul link è possibile scegliere tra IPv4 e IPv6.

Indirizzo IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP desiderato.

Consenti connessione a desktop remoto

Consente le connessioni "Remote-Desktop" (protocollo Remote Desktop) sulla Porta 3389

Porta

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la porta utilizzata per la connessione Remote-Desktop consentita.

Consenti connessione VNC

Consente le connessioni VNC (Virtual Network Computing) sulla Porta 5900

Porta

Facendo clic con il mouse sul link, si apre una finestra di dialogo nella quale è possibile immettere la porta utilizzata per la connessione VNC consentita.

Consenti sblocco file e stampante

Consente l'accesso al rilascio di file e stampanti: traffico dati TCP in ingresso sulla Porta 137, 139 e traffico dati UDP in ingresso sulla Porta 445 da un indirizzo IP di preferenza.

Possibili regole in entrata

- **Regola IP in entrata**
- **Regola ICMP in entrata**
- **Regola UDP in entrata**
- **Regola TCP in entrata**
- **Regola protocollo IP in entrata**

Possibili regole in uscita

- **Regola IP in uscita**
- **Regola ICMP in uscita**
- **Regola UDP in uscita**
- **Regola TCP in uscita**
- **Regola protocollo IP in uscita**

Suggerimenti
Le opzioni delle possibili regole in entrata e delle regole in uscita sono identiche alle opzioni delle regole predefinite del protocollo corrispondente, come descritto in FireWall > Regole adattatore.

Pulsanti

Pulsanti	Descrizione
OK	La regola selezionata viene inserita come nuova Regola adattatore.
Annulla	La finestra si chiude senza che venga aggiunta alcuna nuova regola.

12.5.3 Regole di applicazione

Regole di applicazione per l'utente

Questo elenco contiene tutti gli utenti nel sistema. Qualora ci si registri come Amministratore è possibile selezionare un utente per il quale creare delle regole. Nel caso in cui non si sia in possesso di diritti privilegiati, l'elenco mostrerà esclusivamente l'utente attualmente registrato.

Applicazione

Questa tabella mostra l'elenco delle applicazioni per le quali è stata definita una regola. L'elenco mostra le impostazioni di ogni applicazione che è stata eseguita dall'installazione del FireWall di Avira e per la quale è stata memorizzata una regola.

Visualizzazione standard

Colonna	Descrizione
Applicazione	Nome dell'applicazione
Connessioni attive	Numero delle connessioni attive aperte dall'applicazione

Azione	Visualizza l'azione che il FireWall Avira deve eseguire automaticamente nel caso in cui l'applicazione utilizzi la rete, indipendentemente dall'uso che ne fa. Facendo clic con il mouse sul link si ha la possibilità di passare a un altro tipo di azione. Sono disponibili i tipi di azione **Chiedi**, **Consenti** o **Rifiuta**. L'impostazione standard è **Chiedi**.

Configurazione estesa

Se si desidera regolare individualmente gli accessi alla rete di un'applicazione, è possibile creare, analogamente alle regole adattatore, specifiche regole di applicazione che si basano sui filtri di pacchetto.

- Per passare alla configurazione estesa delle regole di applicazione, attivare dapprima la **Modalità esperto**.
- Successivamente modificare in **Configurazione > Sicurezza Internet > FireWall > Impostazioni** le impostazioni relative alle *regole di applicazione*: Attivare l'opzione **Impostazioni avanzate** e salvare l'impostazione con **Applica** oppure **OK**.
  - ↳ In **Configurazione > Sicurezza Internet > FireWall > Regole di applicazione**, nell'elenco delle regole di applicazione sarà visualizzata un'altra colonna **Filtro** con la voce **Semplice**.

Colonna	Descrizione
Applicazione	Nome dell'applicazione.
Connessioni attive	Numero delle connessioni attive aperte dall'applicazione

Azione	Visualizza l'azione che il FireWall Avira deve eseguire automaticamente nel caso in cui l'applicazione utilizzi la rete, indipendentemente dall'uso che ne fa. Impostando **Filtro - Semplice** è possibile passare a un'altra modalità di azione facendo clic con il mouse sul collegamento. Sono disponibili i tipi di azione **Chiedi**, **Consenti** e **Rifiuta**. Impostando **Filtro - Avanzato** si visualizzerà la modalità di azione **Regole**. Il link **Regole** apre la finestra **Regole di applicazione**, in cui è possibile salvare regole avanzate specifiche per l'applicazione.
Filtro	Permette di visualizzare la modalità di filtro. Facendo clic con il mouse sul link si ha la possibilità di passare a un altro tipo di filtro. **Semplice**: Impostando il filtro semplice l'azione indicata sarà eseguita per tutte le attività di rete dell'applicazione software. **Avanzato**: Il filtro prevede l'esecuzione delle regole salvate nella configurazione estesa.

- Se si desidera impostare le regole di applicazione specificate per un'applicazione, sarà sufficiente passare alla voce **Filtro** all'impostazione **Avanzato**.
  - ↳ Nella colonna **Azione** comparirà quindi la voce **Regole**.
- Fare clic su **Regole** per accedere nella finestra all'impostazione di regole di applicazione specifiche.

Regole di applicazione specifiche della configurazione estesa

Utilizzando regole di applicazione specifiche è possibile consentire o rifiutare il traffico di dati specifico dell'applicazione, nonché consentire o rifiutare l'attesa passiva dalle singole porte. Sono disponibili le seguenti opzioni:

Consenti/rifiuta inserimento di codice

L'inserimento di codice è una tecnica che esegue codice nello spazio indirizzi di un altro processo e obbliga tale processo a caricare una Dynamic Link Library (DLL). Questa tecnica viene utilizzata ad esempio dal malware per eseguire codice sotto la copertura di altri programmi. In questo modo è possibile, ad esempio, nascondere gli accessi Internet al FireWall. In generale l'inserimento di codice è consentito a tutte le applicazioni dotate di firma.

Consenti o rifiuta l'attesa passiva dell'applicazione dalle porte

Consenti o rifiuta il traffico di dati:

Consenti o rifiuta pacchetti IP in ingresso e/o in uscita

Consenti o rifiuta pacchetti TCP in ingresso e/o in uscita

Consenti o rifiuta pacchetti UDP in ingresso e/o in uscita

Per ciascuna applicazione è possibile creare un numero a piacere di regole di applicazione. Le regole di applicazione vengono eseguite nell'ordine visualizzato (ulteriori informazioni sono disponibili in Regole di applicazione estese).

> **Suggerimenti**
> Nel caso in cui il filtro di una regola di applicazione venga modificato da **Avanzato** in **Semplice**, le regole di applicazione già impostate nella configurazione estesa non vengono definitivamente eliminate, ma solo disattivate. Se si passa di nuovo all'azione di filtro **Avanzato**, le regole di applicazione già impostate vengono di nuovo attivate e visualizzate nella finestra della configurazione estesa **Regole di applicazione**.

Dettagli applicazione

In questa categoria vengono visualizzate informazioni dettagliate relative all'applicazione selezionata dall'utente nell'elenco delle applicazioni.

- *Nome* - Nome dell'applicazione.
- *Percorso* - Percorso del file eseguibile dell'applicazione.

Pulsanti

Pulsanti	Descrizione
Aggiungi applicazione	Consente la creazione di una nuova regola di applicazione. Facendo clic su questo pulsante appare una finestra di dialogo. Ora è possibile selezionare un'applicazione per la quale si desidera creare una regola.
Rimuovi regola	Elimina la regola applicazione selezionata.
Inserisci dettagli	Nella finestra *Proprietà* vengono visualizzate informazioni dettagliate relative all'applicazione selezionata dall'utente nell'elenco delle applicazioni. (Opzione disponibile solo in Modalità esperto).
Carica nuovamente	Carica nuovamente la lista delle applicazioni e rifiuta al contempo tutte le modifiche apportate alle regole applicazione.

12.5.4 Regole di applicazione estese

Nella finestra **Regole di applicazione estese** è possibile creare specifiche regole per il traffico di dati delle applicazioni e l'attesa delle porte. È possibile creare una nuova regola con il pulsante **Aggiungi**. Nella parte inferiore della finestra è possibile specificare ulteriormente la regola. Per un'applicazione è possibile creare un numero a piacere di regole. Le regole vengono eseguite nell'ordine visualizzato. Con i pulsanti **In alto** e **In basso** è possibile modificare l'ordine delle regole.

> **Suggerimenti**
> Per modificare la posizione di una regola di applicazione, è possibile trascinare nella posizione desiderata la regola anche utilizzando il mouse.

Dettagli applicazione

Nell'area Dettagli applicazione vengono visualizzate le informazioni relative all'applicazione selezionata:

- *Nome* - Nome dell'applicazione.
- *Percorso* - Percorso del file eseguibile dell'applicazione.

Opzioni regola

Consenti/rifiuta inserimento di codice

Facendo clic con il mouse sul link è possibile decidere se consentire o rifiutare l'inserimento di codice per l'applicazione selezionata

Tipo regola: traffico / attesa

Facendo clic con il mouse sul link è possibile decidere se creare una regola per il traffico di dati o per l'attesa dalle porte.

Azione: Consenti/rifiuta

Facendo clic con il mouse sul link è possibile decidere quale azione viene eseguita con la regola.

Porta

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la porta locale cui fa riferimento la regola di attesa. È possibile immettere anche più porte o sezioni di porte.

Pacchetti in ingresso, in uscita, tutti i pacchetti

Facendo clic con il mouse sul link è possibile decidere se la regola per il traffico monitora tutti i pacchetti, solo quelli in uscita o solo quelli in ingresso.

Pacchetti IP / Pacchetti TCP / Pacchetti UDP

Facendo clic con il mouse sul link è possibile decidere quale protocollo effettua il monitoraggio della regola per il traffico.

Opzioni per i pacchetti IP:

Indirizzo IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP desiderato.

Maschera IP

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la maschera IP desiderata.

Opzioni per i pacchetti TCP/UDP:

Indirizzo IP locale

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP locale desiderato.

Maschera IP locale

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la maschera IP locale desiderata.

Indirizzo IP remoto

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'indirizzo IP remoto desiderato.

Maschera IP remota

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere la maschera IP remota desiderata.

Porta locale

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere una o più porte locali desiderate o anche intere sezioni di porte.

Porta remota

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere una o più porte remote desiderate o anche intere sezioni di porte.

Non scrivere nel file di report / Scrivi nel file di report

Facendo clic con il mouse sul link è possibile decidere se in presenza di una regola viene immessa una voce nel file di report del programma.

Pulsanti

Pulsanti	Descrizione
Aggiungi	Viene creata una nuova regola di applicazione.
Cancella	La regola di applicazione selezionata viene eliminata.
In alto	La regola selezionata viene spostata di una posizione verso l'alto, aumentando in tal modo la priorità della regola.
In basso	La regola di applicazione selezionata viene spostata di una posizione verso il basso, riducendo in tal modo la priorità della regola.
Rinomina	La regola selezionata viene modificata in modo da poter immettere un nuovo nome di regola.
Applica	Le modifiche effettuate vengono memorizzate e utilizzate direttamente tramite il FireWall di Avira.
OK	Le impostazioni effettuate vengono memorizzate. La finestra per la configurazione delle regole di applicazione si chiude.
Annulla	La finestra per la configurazione delle regole di applicazione si chiude, senza memorizzare le modifiche effettuate.

12.5.5 Fornitori affidabili

In *Fornitori affidabili* viene visualizzato un elenco dei produttori di software affidabili. (Opzioni disponibili solo in Modalità esperto).

È possibile rimuovere o aggiungere produttori dall'elenco utilizzando l'opzione **Fidati sempre di questo fornitore** nella finestra di pop up **Evento di rete**. È possibile consentire di default l'accesso alla rete delle applicazioni, dotate della firma dei fornitori contenuti nell'elenco, attivando l'opzione **Consenti automaticamente le applicazioni create da fornitori affidabili**.

Fornitori affidabili per l'utente

Questo elenco contiene tutti gli utenti del sistema. Qualora ci si registri come Amministratore è possibile selezionare un utente il cui elenco di fornitori affidabili si desidera esaminare o gestire. Qualora l'utente non fosse in possesso di diritti privilegiati, l'elenco mostra solamente l'utente attualmente registrato.

Consenti automaticamente applicazioni create da fornitori affidabili

Se l'opzione è attivata, viene consentito automaticamente l'accesso alla rete alle applicazioni dotate della firma dei fornitori conosciuti e affidabili. L'opzione è attivata di default.

Fornitori

L'elenco mostra tutti i fornitori classificati come affidabili.

Pulsanti

Pulsanti	Descrizione
Cancella	La voce contrassegnata viene rimossa dall'elenco dei fornitori affidabili. Per rimuovere definitivamente dall'elenco il fornitore selezionato, fare clic su **Applica** oppure su **OK** nella finestra di configurazione.
Carica nuovamente	Le modifiche effettuate vengono annullate: l'ultimo elenco memorizzato viene caricato.

Suggerimenti
Se si rimuovono fornitori dall'elenco e si fa clic sul pulsante **Applica**, i fornitori vengono definitivamente eliminati dall'elenco. Non è possibile annullare la modifica con **Carica nuovamente**. È tuttavia possibile aggiungere nuovamente un fornitore all'elenco dei fornitori affidabili tramite l'opzione **Fidati sempre di questo fornitore** nella finestra di pop up **Evento di rete**.

Suggerimenti
Il FireWall dà la priorità alle regole di applicazione rispetto alle voci dell'elenco

dei fornitori affidabili: se è stata creata una regole di applicazione e il fornitore dell'applicazione è compreso nell'elenco dei fornitori affidabili, la regola viene eseguita.

12.5.6 Impostazione

Opzioni disponibili solo in Modalità esperto.

Impostazioni aggiuntive

Disattiva Windows Firewall all'avvio

Se l'opzione è attivata, Windows Firewall risulta disattivato all'avvio del computer. Questa opzione è attivata di default.

Timeout della regola

Blocca sempre

Se l'opzione è attivata viene mantenuta una regola che viene creata automaticamente ad esempio durante un Port-Scan.

Rimuovi regola dopo n secondi

Se l'opzione è attivata viene eliminata una regola creata, per esempio, durante un Port-Scan dopo un intervallo definito dall'utente. Questa opzione è attivata di default. Questo campo permette di specificare il numero di secondi in seguito al quale la regola verrà rimossa.

Notifiche

In Notifiche è possibile determinare al verificarsi di quali eventi si desidera ricevere un messaggio del FireWall sul desktop.

Port scan

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rilevato un Port-Scan.

Flooding

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rilevato un attacco flood.

Applicazioni bloccate

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rifiutato o bloccato un'attività di rete di un'applicazione.

IP bloccato

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rifiutato il traffico di dati da un indirizzo IP.

Regole di applicazione

Le opzioni dell'area Regole di applicazione consentono di impostare le possibilità di configurazione delle regole di applicazione nella rubrica FireWall > Regole applicazione.

Impostazioni aggiuntive

Se l'opzione è attivata, è possibile regolare individualmente i diversi accessi alla rete di un'applicazione.

Impostazioni di base

Se l'opzione è attivata, è possibile impostare una sola azione per i diversi accessi alla rete dell'applicazione.

12.5.7 Impostazioni pop up

Opzioni disponibili solo in Modalità esperto.

Verificare lo Startblock del processo

Se l'opzione è attivata, viene verificato accuratamente il batch del processo. Il FireWall parte dal presupposto che ogni processo in batch, mediante il quale il processo figlio interviene sulla rete, non sia affidabile. Pertanto in questo caso viene aperta una finestra pop up per ogni processo in batch non affidabile. Questa opzione è disattivata di default.

Mostra più finestre di dialogo per processo

Se l'opzione è attivata, viene aperta una finestra pop up ogni volta che un'applicazione tenta di creare una connessione a Internet. In alternativa, l'informazione viene presentata solo al primo tentativo di connessione. Questa opzione è disattivata di default.

Memorizza azione per questa applicazione

Sempre attivo

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" è attivata di default.

Sempre disattivato

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" è disattivata di default.

Consenti applicazioni con firma

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" è attivata di default per l'accesso alla rete di applicazioni firmate di produttori specifici. Queste applicazioni con firma vengono messe a disposizione dai cosiddetti "fornitori affidabili" (vedere Fornitori affidabili).

Ricorda stato più recente

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" viene gestita come per l'ultimo evento di rete. Se nell'ultimo evento di rete l'opzione "**Memorizza azione per questa applicazione**" era attivata, risulta attiva anche per gli eventi di rete successivi. Se nell'ultimo evento di rete l'opzione "**Memorizza azione per questa applicazione"** era disattivata, risulta disattivata anche per gli eventi di rete successivi.

Visualizza dettagli

In questo gruppo di opzioni di configurazione è possibile definire la visualizzazione di informazioni dettagliate nella finestra **Evento di rete**.

Visualizza dettagli su richiesta

Se l'opzione è attivata, le informazioni dettagliate nella finestra "**Evento di rete**" vengono visualizzate solo su richiesta, ovvero facendo clic sul pulsante "**Visualizza dettagli**" nella finestra "**Evento di rete**".

Visualizza sempre dettagli

Se l'opzione è attivata, le informazioni dettagliate nella finestra "**Evento di rete**" vengono sempre visualizzate.

Ricorda stato più recente

Se l'opzione è attivata, la visualizzazione delle informazioni dettagliate viene gestita come per l'evento di rete precedente. Se per l'ultimo evento di rete le informazioni dettagliate erano visualizzate o richiamate, anche negli eventi successivi vengono visualizzate. Se per l'ultimo evento di rete le informazioni dettagliate non erano visualizzate o richiamate, anche negli eventi successivi non vengono visualizzate.

12.6 Web Protection

La rubrica **Web Protection** in **Configurazione > Sicurezza Internet** è dedicata alla configurazione di Web Protection.

12.6.1 Cerca

Web Protection consente di proteggersi da virus e malware, che giungono sul computer attraverso i siti Web caricati da Internet nel browser Web. Nella rubrica **Scansione** è

possibile impostare il comportamento di Web Protection. (Opzioni disponibili solo in Modalità esperto).

Cerca

Supporto di IPv6

Se l'opzione è attivata, viene supportata la versione 6 di Web Protection.

Protezione drive-by

La *protezione drive-by* consente di effettuare impostazioni per bloccare gli iframe, detti anche inline frame. Gli iframe sono elementi HTML, ovvero elementi di siti Internet, che delimitano un'area di un sito Web. Gli iframe consentono di caricare e visualizzare altri contenuti Web, per lo più di altri URL, come documenti indipendenti in una sottofinestra del browser. Gli iframe vengono principalmente utilizzati per i banner pubblicitari. In alcuni casi gli iframe vengono utilizzati per nascondere virus e malware. In questi casi l'area dell'iframe nel browser è appena o per niente visibile. L'opzione **Blocca iframe sospetti** consente di controllare e di bloccare il caricamento di iframe.

Blocca I-Frames sospetti

Se l'opzione è attivata, gli iframe dei siti richiesti vengono verificati in base a determinati criteri. Se in uno dei siti Web richiesti sono presenti iframe sospetti, l'iframe viene bloccato. Nella finestra dell'iframe viene visualizzato un messaggio di errore.

Azione per i rilevamenti

È possibile stabilire delle azioni che Web Protection deve eseguire quando viene rilevato un virus o un programma indesiderato. (Opzioni disponibili solo in Modalità esperto.)

Interattivo

Se l'opzione è attivata, durante la scansione diretta in caso di rilevamento di un virus o di un programma indesiderato, viene visualizzata una finestra di dialogo nella quale è possibile scegliere come procedere con i file infetti. Questa opzione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, quando un download o lo scaricamento del contenuto di pagine Websupera un timeout di 20 secondi viene visualizzato un messaggio sul desktop con una barra di progressione per il download. Questo messaggio sul desktop è utile in particolare per il controllo del download da pagine Web con grandi volumi di dati: navigando con Web Protection i contenuti delle pagine Web non vengono caricati gradualmente nel browser Internet poiché, prima di essere visualizzati nel browser Internet vengono scansionati alla ricerca di virus e malware. Questa opzione è disattivata di default.

É possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Web Protection reagisce conformemente alle impostazioni effettuate dall'utente in questa sezione.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Web Protection rileva un virus o un programma indesiderato.

Nega accesso

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso. Web Protection inserisce il rilevamento nel file di report, a condizione che la funzione di report sia attivata.

quarantena

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inviati in quarantena in caso di rilevamento di un virus o di un malware. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

Ignora

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web. L'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Accessi bloccati

In **Accessi bloccati** è possibile immettere i tipi di file e i tipi di MIME (tipi di contenuto dei dati trasmessi) che devono essere bloccati da Web Protection.Il filtro Web consente di bloccare URL noti indesiderati, quali gli URL di phishing e malware. Web Protection impedisce il trasferimento dei file da Internet al computer. (Opzioni disponibili solo in Modalità esperto).

Tipi di file / MIME che Web Protection deve bloccare

Tutti i tipi di file e i tipi di MIME (tipo di contenuto dei dati trasmessi) nell'elenco vengono bloccati da Web Protection.

Campo

In questo campo immettere i nomi dei tipi di MIME e dei tipi di file che devono essere bloccati da Web Protection. Per i tipi di file, inserire l'estensione del file, ad esempio**.htm**. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio**video/mpeg** o **audio/x-wav**.

> **Suggerimenti**
> I file che sono già stati salvati sul computer come file Internet temporanei, vengono bloccati da Web Protection, ma possono comunque venire caricati dal computer localmente dal browser Internet. I file temporanei Internet sono file che vengono memorizzati sul computer dal browser Internet per poter visualizzare le pagine Web più rapidamente.

> **Suggerimenti**
> L'elenco dei tipi di file e dei tipi MIME da bloccare viene ignorato per le voci dell'elenco dei tipi di file e dei tipi MIME da tralasciare in Eccezioni.

> **Suggerimenti**
> Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Tipi di MIME: esempi per tipi di supporto

- `text` = per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `application/octet-stream` = i file del tipo MIME application/octet-stream (eseguibili *.bin, *.exe, *.com, *dll, *.class) vengono bloccati da Web Protection.
- `application/olescript` = i file del tipo MIME application/olescript (file di script ActiveX *.axs) vengono bloccati da Web Protection.
- `.exe` = tutti i file con l'estensione .exe (file eseguibili) vengono bloccati da Web Protection.
- `.msi` = tutti i file con estensione .msi (file di Windows Installer) vengono bloccati da Web Protection.

Aggiungi

Con il pulsante è possibile accettare i MIME e il tipo di file indicati nella finestra.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Filtro Web

Il filtro Web dispone di una banca dati interna aggiornata quotidianamente nella quale gli URL sono classificati in base a criteri di contenuto.

Attiva filtro Web

Se l'opzione è attivata, vengono bloccati tutti gli URL appartenenti alle categorie selezionate nell'elenco del filtro Web.

Elenco filtro Web

Nell'elenco del filtro Web è possibile selezionare le categorie di contenuto i cui URL devono essere bloccati da Web Protection.

Suggerimenti
Il filtro web viene ignorato per le voci dell'elenco degli URL da tralasciare in Eccezioni.

Suggerimenti
Vengono categorizzati come**URL di spam** gli URL diffusi con i messaggi email di spam. La categoria **Frode/Inganno** comprende i siti web con 'abbonamenti-trappola' e altre offerte di servizi i cui costi vengono occultati dal fornitore.

Eccezioni

Queste opzioni consentono di escludere tipi di MIME (tipi di contenuto dei file trasferiti) e tipi di file per gli URL (indirizzi Internet) dalla scansione di Web Protection. Gli URL e i tipi di MIME indicati vengono ignorati da Web Protection, ovvero durante la trasmissione al computer dell'utente non viene effettuata la scansione di questi dati per verificare la presenza di virus e malware (opzioni disponibili solo in Modalità esperto).

Tipi di MIME da omettere da Web Protection

In questo campo è possibile selezionare tipi di MIME (tipi di contenuto dei dati trasferiti) che devono essere esclusi dalla scansione di Web Protection.

Tipi di file / tipi di MIME da escludere da Web Protection (definiti dall'utente)

Tutti i tipi di file e i tipi di MIME (tipi di contenuto dei dati trasferiti) nell'elenco vengono esclusi dalla scansione di Web Protection.

Campo

Inserire in questo campo i nomi dei tipi di MIME e di file che si intendono escludere dalla scansione di Web Protection. Per i tipi di file, inserire l'estensione del file, ad esempio `.htm`. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio`video/mpeg` oppure `audio/x-wav`.

Suggerimenti
Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Attenzione
Tutti i tipi di file e di contenuto nell'elenco delle eccezioni vengono caricati nel browser Internet senza ulteriori verifiche di blocco dell'accesso (elenco dei tipi di file e di MIME da bloccare in Accesso bloccato) o di Web Protection: Per tutte le voci dell'elenco delle eccezioni viene ignorato il contenuto dell'elenco dei tipi di file e di MIME da bloccare. Non viene eseguita alcuna scansione per virus e malware.

Tipi di MIME: esempi per tipi di supporto

- `text` per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `audio/` = tutti i file del tipo di supporto audio vengono esclusi dalla scansione di Web Protection
- `video/quicktime` = tutti i file video del sottotipo Quicktime (*.qt, *.mov) vengono esclusi dalla scansione di Web Protection
- `.pdf` = tutti i file Adobe-PDF vengono esclusi dalla scansione di Web Protection.

Aggiungi

Con il pulsante è possibile accettare i MIME e il tipo di file indicati nella finestra.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

URL da omettere da Web Protection

Tutti gli URL di questo elenco vengono esclusi dalla scansione di Web Protection.

Campo

Immettere in questo campo gli URL (indirizzi Internet) che devono essere esclusi dalla scansione di Web Protection, ad es.**www.domainname.com**. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: .domainname.it per tutte le pagine e i tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: **domainname.**. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net).

Suggerimenti
Nell'immissione degli URL è possibile utilizzare anche wildcard * per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (valido ma non consigliato)
I dati senza punti quali `*name*` vengono interpretati come parti di dominio di livello superiore e non sono consigliati.

Attenzione
Tutte le pagine web dell'elenco degli URL da escludere vengono caricati nel browser Internet senza ulteriori verifiche del filtro Web o di Web Protection : per tutte le voci dell'elenco degli URL da tralasciare vengono ignorate le voci del filtro Web (vedere Accesso bloccato). Non viene eseguita alcuna scansione per virus e malware. Si consiglia pertanto di escludere dalla scansione di Web Protection solo URL affidabili.

Aggiungi

Con il pulsante è possibile accettare nella finestra gli URL (indirizzi Internet) indicati.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Esempi: URL da tralasciare

- `www.avira.com` -O- `www.avira.com/*`
  = Tutti gli URL con dominio 'www.avira.com' vengono esclusi dalla scansione di Web Protection: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,.. Gli URL con dominio www.avira.com/it vengono esclusi dalla scansione di Web Protection.
- `avira.com` -O- `*.avira.com`
  = Tutti gli URL con dominio di livello secondario o superiore 'avira.com' vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini secondari esistenti di '.avira.com': www.avira.com, forum.avira.com,...
- `avira.` -O- `*.avira.*`
  = Tutti gli URL con dominio di livello secondario 'avira' vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di '.avira.': www.avira.com, www.avira.com/it, forum.avira.com,...
- `.*domain*.*`
  = Tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri 'domain', vengono esclusi dalla scansione di Web Protection: www.domain.com, www.new-domain.it, www.sample-domain1.it, ...
- `net` -O- `*.net`
  = Tutti gli URL con dominio di livello superiore 'net' vengono esclusi dalla scansione di Web Protection: www.name1.net, www.name2.net,...

> **Attenzione**
> Indicare tutti gli URL che si desidera escludere dalla scansione di Web Protection nel modo più preciso possibile. Evitare l'immissione di tutti i domini di livello superiore o parti di nomi di domini secondari, poiché vi è il rischio che le pagine Internet, che diffondono malware e programmi indesiderati mediante dati globali, vengano escluse dalla scansione di Web Protection come eccezione. Si consiglia di immettere almeno il dominio secondario e il dominio di livello superiore completi: domainname.com

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzioni disponibili solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta

all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il prodotto Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

12.6.2 Child Protection

Il programma Avira è provvisto di una funzione di protezione bambini per filtrare offerte Internet indesiderate o illegali e per la limitazione temporale dell'utilizzo di Internet. La funzione di protezione bambini fa parte del componente Web Protection.

È possibile assegnare ruoli utente agli utenti del computer. I ruoli utente sono configurabili e comprendono un set di regole con i seguenti criteri:

- URL consentiti o non consentiti (indirizzi Internet)
- Categorie di contenuti non consentite
- Durata dell'utilizzo di Internet ed eventuali intervalli di tempo consentiti per l'utilizzo nei giorni della settimana

Per bloccare i contenuti Internet in base a determinate categorie vengono utilizzati elenchi di filtri URL efficaci, nei quali gli URL vengono categorizzati in gruppi di contenuti in base ai contenuti delle pagine Internet. Gli elenchi dei filtri URL vengono aggiornati, adattati e

ampliati più volte ogni ora. I ruoli **bambino**, **adolescente**, **adulto** sono preconfigurati con le categorie non consentite corrispondenti.

L'utilizzo temporale di Internet viene stabilito sulla base di richieste di collegamento a Internet che avvengono con un intervallo minimo di 5 minuti.

Se la protezione bambini è attivata, durante la navigazione in Internet tutti i siti Web richiesti nel browser vengono verificati in base al ruolo utente. In caso di siti Web non consentiti, il sito Web viene bloccato e viene visualizzato un messaggio nel browser. In caso di superamento della durata di utilizzo consentita oppure se l'utilizzo supera l'intervallo consentito, le pagine Web richiamate vengono bloccate. Nel browser viene visualizzato un messaggio.

> **Attenzione**
> Si osservi che è necessario attivare il servizio Web Protection per poter utilizzare la funzione protezione bambini.

> **Attenzione**
> Quando si attiva la protezione bambini, proteggere la configurazione del prodotto Avira mediante una password. Se la configurazione non è protetta tramite password, tutti gli utenti del computer potranno modificare o disattivare le impostazioni della protezione bambini. È possibile attivare la password in Configurazione > Generale > Password.

Se è stata assegnata una password per la protezione bambini, la configurazione per la protezione bambini viene nascosta e viene visualizzato il pulsante **Protetto da password**.

Protetto da password

Fare clic sul pulsante "**Protetto da password"** e inserire la password per la protezione bambini nella finestra "**Inserimento password**" per abilitare la configurazione della protezione bambini.

Attiva protezione bambini

Se l'opzione è attivata, tutti i siti web, richiesti durante la navigazione in Internet, vengono verificati in base al ruolo assegnato all'utente registrato nella protezione per bambini. I siti web richiesti vengono bloccati se sono stati classificati come non consentiti nell'ambito del ruolo assegnato.

> **Suggerimenti**
> Se la protezione bambini è attivata, l'utente del computer al quale non è stato assegnato alcun ruolo nella configurazione della protezione bambini viene classificato di default dal programma come *Standard* con il ruolo **Bambino**. È possibile modificare il ruolo dell'utente standard.

Dopo l'installazione vengono applicati i ruoli utente **bambino**, **adolescente** e **adulto**. Nei ruoli preconfigurati, la limitazione temporale dell'utilizzo di Internet è disattivata.

Selezione utente

Utente

L'elenco contiene tutti gli utenti del sistema.

Aggiungi

Il pulsante consente di aggiungere l'utente selezionato all'elenco degli utenti protetti.

Elimina

Il pulsante consente di eliminare la voce dell'elenco selezionata.

Elenco utenti - Ruolo

Nell'elenco vengono visualizzati tutti gli utenti con il relativo ruolo assegnato. Quando si aggiunge un utente, il programma assegna di default il ruolo **Bambino**. Facendo clic con il mouse sul ruolo visualizzato, è possibile passare a un altro ruolo.

Suggerimenti
Non è possibile eliminare l'utente *standard*.

Ruoli(Opzioni disponibili solo in Modalità esperto).

Campo

Immettere nel campo il nome del ruolo che si desidera aggiungere ai ruoli utente.

Modifica

Il pulsante "**Modifica**" consente di configurare il ruolo selezionato. Viene visualizzata una finestra di dialogo nella quale è possibile definire per il ruolo URL consentiti e non consentiti e contenuti web non consentiti in base a categorie. (vedere Proprietà del ruolo)

Aggiungi

Il pulsante consente di aggiungere all'elenco dei ruoli disponibili il ruolo immesso nel campo.

Elimina

Il pulsante consente di eliminare dall'elenco il ruolo selezionato.

Elenco

Nell'elenco vengono visualizzati tutti i ruoli immessi. Facendo doppio clic su un ruolo, si apre la finestra di dialogo per la definizione del ruolo.

> **Suggerimenti**
> Non è possibile eliminare i ruoli già assegnati a un utente.

Proprietà del ruolo

Nella finestra **Proprietà del ruolo** è possibile definire un ruolo selezionato per l'utilizzo di Internet. (Opzioni disponibili solo in Modalità esperto).

È possibile consentire o non consentire esplicitamente l'accesso agli URL. È possibile bloccare i contenuti Web in base alla selezione di determinate categorie. È possibile limitare temporalmente l'utilizzo di Internet.

Controlla l'accesso agli URL seguenti

Nell'elenco vengono visualizzati tutti gli URL immessi con le regole assegnate *Blocca* o *Consenti*. Quando si aggiunge un URL, viene assegnata di default la regola *Blocca*. Facendo clic sulla regola è possibile cambiare la regola assegnata.

Aggiungi URL

Immettere nel campo gli URL che devono essere controllati dalla funzione di protezione bambini. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: **.domainname.it** per tutte le pagine e tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: domainname.. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net). È possibile utilizzare anche il metacarattere ***** per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard.

> **Suggerimenti**
> Alle regole URL viene data la priorità in base al numero delle parti di nome immesse (label) del dominio. Tante più parti di nome si immettono per il dominio, tanto maggiore sarà la priorità della regola. Es.:
> URL: www.avira.com - Regola: Consenti
> URL: .avira.com - Regola: Blocca
> Il set di regole consente tutti gli URL del dominio 'www.avira.com'. L'URL 'forum.avira.com' viene bloccato.

> **Suggerimenti**
> Immettendo . oppure * vengono compresi tutti gli URL. Utilizzare tali caratteri se

si desidera consentire, ad esempio per il ruolo *Bambino*, solo pochi siti web indicati in modo esplicito, ad es. nel seguente set di regole:
URL: ***** o **.** - Regola: Blocca
URL: kids.yahoo.com - Regola: Consenti
URL: kids.nationalgeographic.com - Regola: Consenti
Il set di regole blocca tutti gli URL tranne gli URL con i domini "kids.yahoo.com" e "kids.nationalgeographic.com".

Aggiungi

Il pulsante consente di aggiungere all'elenco degli URL controllati l'URL immesso.

Elimina

Il pulsante consente di eliminare dall'elenco degli URL controllati l'URL selezionato.

Blocca l'accesso agli URL appartenenti alle categorie seguenti

Se l'opzione è attivata, vengono bloccati i contenuti Web appartenenti alle categorie selezionate del relativo elenco.

Durata utilizzo consentita

Con il pulsante **Durata utilizzo consentita** si apre una finestra di dialogo in cui è possibile impostare una limitazione temporale all'utilizzo di Internet per il ruolo che si sta configurando. È possibile stabilire l'utilizzo di Internet mensile, settimanale, oppure differenziato a seconda che si tratti di giorni infrasettimanali o del weekend. Nella finestra di dialogo successiva è possibile stabilire gli intervalli di tempo precisi per ogni giorno della settimana. Vedere Durata utilizzo.

Esempi: URL da controllare

- `www.avira.com` -O- `www.avira.com/*`
  = Comprende tutti gli URL con il dominio `www.avira.com`: *www.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*,..
  Non sono compresi URL con il dominio www.avira.com/it.
- `avira.com` -O- `*.avira.com`
  = Comprende tutti gli URL con dominio di livello secondario o superiore `avira.com`. Tali dati comprendono tutti i domini secondari esistenti di `.avira.com`: *www.avira.com*, *forum.avira.com*,...
- `avira.` -O- `*.avira.*`
  = Comprende tutti gli URL con dominio di livello secondario `avira`. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di `.avira.`: *www.avira.com, www.avira.de, forum.avira.com*,...
- `.*domain*.*`
  Comprende tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri '`domain`': *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...

- `net` -O- `*.net`
  =Comprende tutti gli URL con dominio di livello superiore '`net`': *www.name1.net*, *www.name2.net*,...

Durata utilizzo

Nella finestra **Durata utilizzo** è possibile definire una durata massima dell'utilizzo di Internet per un ruolo utente. L'utilizzo temporale di Internet viene stabilito sulla base di richieste di collegamento a Internet che avvengono con un intervallo minimo di 5 minuti. Per ogni ruolo può essere indicato il tempo di navigazione massimo desiderato settimanale, mensile, oppure differenziato a seconda che si tratti di giorni infrasettimanali o del weekend.

Limita temporalmente utilizzo Internet

Questa opzione consente di limitare la durata dell'utilizzo di Internet per tutti gli utenti a cui è assegnato il ruolo. In caso di superamento della durata di utilizzo consentita, le pagine Web richieste, ovvero richiamate, dall'utente vengono bloccate. Nel browser Web compare un avviso.

Limitazione temporale per settimana, mese, giorno (lu-ve, sa-do)

È possibile indicare la durata di utilizzo desiderata mediante il cursore di riempimento o i tasti freccia a destra del campo. Inoltre, la durata di utilizzo può essere impostata direttamente nei campi temporali. A tal fine si osservi il formato indicato per l'indicazione temporale.

Le indicazioni diverse per la durata di utilizzo non vengono uniformate dal programma. Il programma utilizza ogni volta il valore adatto più basso per limitare la durata di utilizzo.

Intervallo di tempo preciso

Con il pulsante **Intervallo di tempo preciso** si apre una finestra di dialogo in cui è possibile stabilire gli orari giornalieri per la durata di utilizzo massima definita. Vedere Intervallo di tempo dell'utilizzo.

Intervallo di tempo dell'utilizzo

Nella finestra **Intervallo di tempo dell'utilizzo** è possibile definire i tempi di utilizzo consentiti per la durata massima dell'utilizzo di Internet indicata per un ruolo: è possibile stabilire determinati orari per l'utilizzo di Internet per ogni giorno della settimana.

Consenti utilizzo di Internet solo agli orari indicati

Questa opzione consente di stabilire gli orari di "navigazione" per tutti gli utenti a cui è assegnato il ruolo configurato. Se gli utenti del computer utilizzano Internet al di fuori degli orari consentiti, le pagine Web richiamate vengono bloccate. Nel browser Web compare un messaggio.

- Per stabilire gli orari dell'utilizzo di Internet, contrassegnare gli intervalli di tempo desiderati.

Vi sono le seguenti possibilità di contrassegnare gli orari autorizzati o bloccati:

- **Per stabilire gli orari dell'utilizzo di Internet:** fare clic sui campi temporali non contrassegnati desiderati o fare clic con il tasto sinistro del mouse sui campi temporali non contrassegnati.
- **Per bloccare gli orari dell'utilizzo di Internet:** fare clic sui campi temporali contrassegnati desiderati o fare clic con il tasto sinistro del mouse sui campi temporali contrassegnati.

- Fare clic con il tasto destro del mouse sui campi temporali del giorno desiderato per richiamare in una finestra di dialogo gli intervalli di tempo indicati. Esempio: *Utilizzo di Internet bloccato da 00:00 alle 11:00.*

12.6.3 Report

Web Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Web Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Web Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, Web Protection registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Web Protection registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione fissata di 50 Kilobyte, vengono

automaticamente eliminate le voci più vecchie fin quando non si raggiunge una dimensione inferiore del 20%.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

> **Suggerimenti**
> Se non sono state specificate limitazioni per i file di report, vengono automaticamente eliminate le voci più vecchie quando il file di report raggiunge le dimensioni di 100 MB. Viene eliminato un numero di voci tali da consentire al file di report di raggiungere una dimensione di 80 MB.

12.7 Mail Protection

La rubrica Mail Protection della configurazione è dedicata alla configurazione di Mail Protection.

12.7.1 Cerca

Mail Protection viene utilizzato per verificare la presenza di virus, malware e spam nelle email in ingresso. Nelle email in uscita, Mail Protection verifica la presenza di virus e malware. Le email in uscita, inviate da un Bot sconosciuto per la diffusione di spam sul computer dell'utente, possono essere bloccate da Mail Protection.

Attiva Mail Protection

Se l'opzione è attivata, il traffico di email viene sottoposto a controlli tramite Mail Protection. Mail Protection è un server proxy che controlla il traffico di dati fra il server email utilizzato e il programma email client sul sistema: Nell'impostazione di default, vengono ricercati malware nelle email in entrata. Se l'opzione è disattivata, il servizio di Mail Protection rimane attivo, tuttavia, il monitoraggio tramite Mail Protection è disattivato.

Scansiona email in entrata

Se l'opzione è attivata, nelle email in entrata viene verificata la presenza di virus, malware e spam . Mail Protection supporta i protocolli POP3 e IMAP. Attivare l'account di posta in entrata, utilizzato dal client email dell'utente per ricevere le email, per il monitoraggio mediante Mail Protection.

Controlla account POP3

Se l'opzione è attivata, gli account POP3 vengono monitorati alla porte in ingresso.

Porte controllate

Immettere nel campo la porta utilizzata per la posta in ingresso dal protocollo POP3. Più porte vengono indicate separate da una virgola. (Opzione disponibile solo in Modalità esperto).

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di POP3. (Opzione disponibile solo in Modalità esperto).

Controlla account IMAP

Se l'opzione è attivata, gli account IMAP vengono monitorati alla porte in ingresso.

Porte controllate

Immettere nel campo la porta utilizzata dal protocollo IMAP. Più porte vengono indicate separate da una virgola. (Opzione disponibile solo in Modalità esperto).

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di IMAP. (Opzione disponibile solo in Modalità esperto).

Scansiona email in uscita (SMTP)

Se l'opzione è attivata, nelle email in uscita viene verificata la presenza di virus e malware. Le email inviate da Bot sconosciuti per la diffusione di spam vengono bloccate.

Porte controllate

Immettere nel campo la porta utilizzata per la posta in uscita dal protocollo SMTP. Più porte vengono indicate separate da una virgola. (Opzione disponibile solo in Modalità esperto).

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di SMTP. (Opzione disponibile solo in Modalità esperto).

> **Suggerimenti**
> Per verificare le porte e i protocolli utilizzati, richiamare le proprietà degli account di posta elettronica nel programma email client utilizzato. Vengono principalmente utilizzate porte standard.

Supporto di IPv6

Se l'opzione è attivata, Mail Protection supporta la versione 6 del protocollo Internet.

Azione per i rilevamenti

Questa rubrica di configurazione contiene le impostazioni delle azioni da intraprendere quando Mail Protection rileva un virus o un programma indesiderato in un'email o in un allegato. (Opzioni disponibili solo in Modalità esperto).

> **Suggerimenti**
> Le azioni definite qui vengono eseguite sia in caso di rilevamento di un virus nelle email in ingresso che nelle email in uscita.

Interattivo

Se l'opzione è attivata, in caso di rilevamento di un virus o di un programma indesiderato in un'email o in un allegato appare una finestra di dialogo nella quale si può selezionare come procedere con l'email o con l'allegato infetto. Questa opzione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, durante il download delle email Mail Protection mostra una barra di progressione. É possibile attivare questa opzione è possibile solo se è stata selezionata l'opzione **Interattivo**.

Automatico

Se l'opzione è attivata, non viene più segnalato il rilevamento di un virus o di un programma indesiderato. Mail Protection reagisce conformemente alle impostazioni effettuate dall'utente in questa sezione.

Email infette

L'opzione selezionata in "*Email infette*" verrà eseguita come azione primaria quando Mail Protection rileva un virus o un programma indesiderato in un'email. Se è stata selezionata l'opzione "**Ignora"** in "*Allegati infetti*", è possibile scegliere come procedere in caso di un rilevamento in un allegato.

Elimina

Se l'opzione è attivata, l'email infetta viene automaticamente eliminata in caso di rilevamento di un virus o di un programma indesiderato. Il corpo dell'email (body) viene sostituito dal testo standard indicato di seguito. Lo stesso vale per gli allegati (Attachments); anche questi ultimi vengono sostituiti da un testo standard.

Ignora

Se l'opzione è attivata, l'email infetta viene ignorata nonostante il rilevamento di un virus o di un programma indesiderato. Si ha tuttavia la possibilità di decidere come procedere con un allegato infetto.

Sposta in quarantena

Se l'opzione è attivata, l'email completa, inclusi gli allegati, viene collocata in Quarantena in caso di rilevamento di virus e programmi indesiderati. Successivamente

- se lo si desidera - può essere ripristinata. Le email infette vengono eliminate. Il corpo dell'email (body) viene sostituito dal testo standard indicato di seguito. Lo stesso vale per gli allegati (Attachments); anche questi ultimi vengono sostituiti da un testo standard.

Allegati infetti

L'opzione "**Allegati infetti**" è selezionabile solo se in "*Email infette*" è stata selezionata l'impostazione "**Ignora**". Con questa opzione si può decidere come procedere in caso di rilevamento in un allegato.

Elimina

Se l'opzione è attivata, in caso di rilevamento di un virus o di un programma indesiderato l'allegato infetto viene eliminato e sostituito con un Testo standard.

Ignora

Se l'opzione è attivata, l'allegato infetto viene ignorato e inoltrato nonostante il rilevamento di un virus o di un programma indesiderato.

Attenzione
Se si seleziona questa opzione non si usufruisce di alcuna protezione da parte di Mail Protection contro virus e programmi indesiderati. Effettuare questa scelta solo se si è sicuri di quello che si sta facendo. Disattivare l'anteprima nel programma email, non aprire mai gli allegati facendo doppio clic!

Sposta in quarantena

Se l'opzione è attivata, l'allegato infetto viene collocato in Quarantena e infine eliminato (sostituito con un testo standard). Successivamente - se lo si desidera - l'allegato può essere ripristinato.

Altre azioni

Questa rubrica di configurazione contiene ulteriori impostazioni delle azioni da intraprendere quando Mail Protection rileva un virus o un programma indesiderato in un'email o in un allegato. (Opzioni disponibili solo in Modalità esperto).

Suggerimenti
Le azioni qui impostate vengono eseguite solo se viene rilevato un virus nelle email in ingresso.

Testo standard per email eliminatee spostate

Il testo in questo campo viene sostituito all'email infetta come notifica nel messaggio. Tale messaggio è modificabile. Può contenere un numero massimo di 500 caratteri.

Per la formattazione si possono utilizzare le seguenti combinazioni di tasti:

Ctrl + Invio = Aggiunge un'interruzione di riga.

Standard

Il pulsante inserisce un testo standard predefinito nel campo.

Testo standard per allegati eliminatie spostati

Il testo in questo campo viene sostituito all'allegato infetto come notifica nell'email. Tale messaggio è modificabile. Può contenere un numero massimo di 500 caratteri.

Per la formattazione si possono utilizzare le seguenti combinazioni di tasti:

Ctrl + Invio = Aggiunge un'interruzione di riga.

Standard

Il pulsante inserisce un testo standard predefinito nel campo.

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzioni disponibili solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il prodotto Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa opzione è attivata di default, se è stata scelta l'applicazione di questa euristica. Questa impostazione è attivata di default e viene consigliata.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

AntiBot

La funzione AntiBot di Mail Protection consente di evitare che il computer venga sfruttato per la diffusione di email di spam all'interno di una cosiddetta Bot-Net: per la diffusione di spam tramite una Bot-Net, di norma un aggressore infetta diversi computer con un bot, che si collega a un server IRC, utilizza un canale specifico e qui attende il comando di invio delle email di spam. Per differenziare le email di spam di un bot sconosciuto da quelle dell'utente, Mail Protection verifica se il server SMTP utilizzato e il mittente dell'email in uscita si trovano nell'elenco dei server e dei mittenti autorizzati. In caso contrario, l'email in uscita viene bloccata, ovvero non viene inviata. L'email bloccata viene segnalata in una finestra di dialogo. (Opzioni disponibili solo in Modalità esperto).

> **Suggerimenti**
> La funzione AntiBot può essere utilizzata solo se la scansione di Mail Protection è attiva per le email in uscita (vedere l'opzione **Scansione email in uscita** in Mail Protection > Scansione).

Server consentiti

Tutti i server in questo elenco sono autorizzati da Mail Protection all'invio di email: le email inviate a questi server **non** vengono bloccate da Mail Protection. Se l'elenco non contiene alcun server, nelle email in uscita non viene verificato il server SMTP utilizzato. Se l'elenco contiene delle voci, Mail Protection blocca le email inviate a un server SMTP che non è presente nell'elenco.

Campo

In questo campo vengono immessi il nome host e l'indirizzo IP del server SMTP utilizzato per l'invio delle email.

> **Suggerimenti**
> I dati relativi ai server SMTP utilizzati dal programma email per l'invio delle email sono riportati all'interno del programma email nei dati dell'account utente impostati.

Aggiungi

Il pulsante consente di aggiungere il server inserito nel campo all'elenco dei server autorizzati.

Elimina

Il pulsante elimina una voce selezionata dall'elenco dei server autorizzati. Questo pulsante non è attivo se non è selezionata alcuna voce.

Elimina tutti

Il pulsante elimina tutte le voci dell'elenco dei server autorizzati.

Mittenti consentiti

Tutti i mittenti in questo elenco sono autorizzati da Mail Protection all'invio di email: le email inviate da questi indirizzi email **non** vengono bloccate da Mail Protection. Se l'elenco non contiene alcun mittente, nelle email in uscita non viene verificato l'indirizzo email del mittente. Se l'elenco contiene delle voci, Mail Protection blocca le email inviate da mittenti non presenti nell'elenco.

Campo

In questo campo immettere gli indirizzi email dei mittenti.

Aggiungi

Il pulsante consente di aggiungere il mittente inserito nel campo all'elenco dei mittenti autorizzati.

Elimina

Il pulsante elimina una voce selezionata dall'elenco dei mittenti autorizzati. Questo pulsante non è attivo se non è selezionata alcuna voce.

Elimina tutti

Il pulsante elimina tutte le voci dall'elenco dei mittenti autorizzati.

12.7.2 Generale

Eccezioni

Indirizzi email non verificati

Questa tabella mostra l'elenco di indirizzi email esclusi dalla scansione di Avira Mail Protection (white list).

Suggerimenti
L'elenco delle eccezioni viene utilizzato da Mail Protection esclusivamente per le email in ingresso.

Campo

Inserire in questo campo gli indirizzi email che si desidera aggiungere all'elenco degli indirizzi email da non controllare. L'indirizzo email non verrà più controllato da Mail Protection in futuro - in base alle impostazioni dell'utente.

Suggerimenti
Quando si immettono indirizzi email si possono utilizzare wildcard: wildcard ***** per il numero di caratteri desiderato e wildcard **?** per un solo carattere. Tuttavia le wildcard possono essere utilizzate solo per gli indirizzi email che non devono essere verificati per lo spam. Se si tenta di escludere dalla verifica del malware un indirizzo con metacaratteri viene visualizzato un messaggio di errore, mentre è stata selezionata la casella di controllo **Malware** nell'elenco delle esclusioni. Nell'immettere indirizzi con wildcard assicurarsi che alla sequenza indicata corrisponda la struttura di un indirizzo email (*@*.*).

Attenzione
Nell'utilizzo di wildcard, considerare gli esempi riportati. Impostare esclusivamente wildcard mirate e verificare con attenzione gli indirizzi email da inserire nella white list per lo spam con l'immissione di wildcard.

Esempi: utilizzo di wildcard negli indirizzi email (white list per lo spam)

- `virus@avira.* /` = raggruppa tutte le email con questo indirizzo e con il dominio di livello superiore desiderato: virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = raggruppa tutte le email inviate dal dominio **avira.com**: info@avira.com, virus@avira.com, kontakt@avira.com, mitarbeiter@avira.com
- `info@*.com` = raggruppa tutti gli indirizzi email con il dominio di livello superiore **com** e l'indirizzo **info**: il dominio di secondo livello è libero: info@name1.com, info@name2.com,...

Aggiungi

Con il pulsante è possibile aggiungere alla lista degli indirizzi email da non verificare un indirizzo email indicato nel campo.

Elimina

Il pulsante elimina un indirizzo email contrassegnato dall'elenco.

Indirizzo email

Indirizzo email che non deve più essere scansionato.

Malware

Se l'opzione è attivata, l'indirizzo email non viene più sottoposto a controlli per malware.

Spam

Se l'opzione è attivata, l'indirizzo email non viene più sottoposto a controlli antispam.

in alto

Questo pulsante consente di spostare un indirizzo email selezionato di una posizione verso l'alto. Il pulsante non è attivo se non è selezionata alcuna voce o se l'indirizzo contrassegnato si trova già nella prima posizione dell'elenco.

in basso

Questo pulsante consente di spostare un indirizzo email selezionato di una posizione verso il basso. Il pulsante non è attivo se non è selezionata alcuna voce o se l'indirizzo contrassegnato si trova già nell'ultima posizione dell'elenco.

Importa rubrica di Outlook

Il pulsante consente di importare indirizzi email dalla rubrica del programma di posta elettronica MS Outlook nell'elenco delle eccezioni. Negli indirizzi email importati non viene verificata la presenza di spam.

Importa rubrica di Outlook Express

Il pulsante consente di importare gli indirizzi email dalla rubrica del programma di posta elettronica MS Outlook Express nell'elenco delle eccezioni. Negli indirizzi email importati non viene verificata la presenza di spam.

Memoria temporanea

La memoria temporanea di Mail Protection contiene i dati relativi alle email scansionate che vengono visualizzati nella statistica del Control Center in **Mail Protection**. (Opzioni disponibili solo in Modalità esperto).

Inoltre, le copie delle email in entrata possono essere archiviate nella memoria temporanea. Le email vengono utilizzate per le funzioni di training (*email buona - utilizza per training*, *spam - utilizza per training*) del modulo AntiSpam.

> **Suggerimenti**
> Per salvare le email in entrata nella memoria temporanea, il modulo AntiSpam deve essere attivato.

Numero massimo di email nella memoria temporanea

In questo campo viene indicato il numero massimo di email che Mail Protection conserva nella memoria temporanea. Vengono eliminate le email più vecchie.

Memorizzazione massima di un'email in giorni

In questo campo viene inserita la durata massima della memorizzazione di un'email in giorni. Dopo questo tempo, l'email viene eliminata dalla memoria temporanea.

Svuota memoria temp.

Facendo clic sul pulsante vengono eliminate le email che vengono conservate nella memoria temporanea.

AntiSpam

Avira Mail Protection scansiona le email alla ricerca di virus e programmi indesiderati. Inoltre, Mail Protection offre una protezione affidabile contro lo spam. (Opzioni disponibili solo in Modalità esperto).

Attiva modulo AntiSpam

Se l'opzione è attivata, la funzione antispam di Mail Protection viene attivata.

Seleziona oggetto email

Se l'opzione è attivata, quando viene rilevata un'email di spam viene aggiunta una nota all'oggetto originario dell'email.

Semplice

Viene aggiunta una nota all'oggetto di un'email di spam o di phishing: [SPAM] o [Phishing]. Questa opzione è attivata di default.

Dettagliato

All'oggetto di un'email spam o di phishing viene aggiunta una nota sulla probabilità che si tratti di spam.

Registra

Se l'opzione è attivata, Mail Protection crea uno speciale file di report AntiSpam.

Utilizza blacklist in tempo reale (RBL)

Se l'opzione è attivata, viene esaminata in tempo reale una cosiddetta "black list" che mette a disposizione informazioni aggiuntive per classificare come spam le email di origine dubbia.

Timeout: n secondo(i)

Se le informazioni di una blacklist non è disponibile dopo n secondi, viene interrotto il tentativo di richiamare la blacklist.

Elimina la banca dati training

Facendo clic sul pulsante vengono eliminate le banche dati training.

Aggiungi automaticamente alla white list il destinatario della email in uscita

Se l'opzione è attivata, gli indirizzi dei destinatari delle email in uscita vengono inseriti automaticamente nella white list dello spam (elenco di email che non vengono verificate per lo spam in **Mail Protection > Generale > Eccezioni**). Le email in ingresso che provengono da indirizzi della white list dello spam non vengono verificate per lo spam. Viene comunque verificata la presenza di virus e malware. Questa opzione è disattivata di default.

> **Suggerimenti**
> Questa opzione può essere attivata solo se la scansione di Mail Protection è attiva per le email in uscita (vedere l'opzione **Scansione email in uscita** in Mail Protection > Scansione).

Piè di pagina

In **Piè di pagina** è possibile configurare un piè di pagina che verrà visualizzato nelle email inviate dall'utente. (Opzioni disponibili solo in Modalità esperto).

Il presupposto per questa funzione è l'attivazione del controllo Mail Protection per le email in uscita; vedere l'opzione **Scansione email in uscita (SMTP)** in **Configurazione > Mail Protection > Scansione**. È possibile utilizzare il piè di pagina definito di Avira Mail Protection con il quale si conferma che l'email inviata è stata controllata da un programma antivirus. È anche possibile immettere un testo per un piè di pagina personalizzato. Se vengono utilizzate entrambe le opzioni come piè di pagina, il testo personalizzato viene anteposto al piè di pagina di Avira Mail Protection.

Piè di pagina nelle email da inviare

Mail Protection > Allega piè di pagina

Se l'opzione è attivata, viene visualizzato il piè di pagina Avira Mail Protection nel testo del messaggio delle email inviate. Con il piè di pagina di Avira Mail Protection si conferma che l'email inviata è stata controllata da Avira Mail Protection per virus e programmi indesiderati e che non proviene da un bot sconosciuto. Il piè di pagina di Avira Mail Protection contiene il testo seguente: "*Scansionato con Avira Mail Protection [versione del prodotto] [abbreviazione del nome e numero versione del motore di ricerca] [abbreviazione del nome e numero versione del file di definizione dei virus]*".

Allega questo piè di pagina

Se l'opzione è attivata, il testo indicato nel campo viene visualizzato come piè di pagina.

Campo

In questo campo è possibile immettere un testo che viene visualizzato come piè di pagina nelle email inviate.

12.7.3 Report

Mail Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Mail Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Mail Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, Mail Protection registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Mail Protection registra nel file di report tutte le informazioni.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata il file del report viene salvato prima dell'abbreviazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione di Mail Protection utilizzata viene riportata nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

12.8 Generale

12.8.1 Categorie di minacce

Selezione delle categorie estese delle minacce (Opzioni disponibili solo in Modalità esperto).

Il prodotto Avira protegge dai virus del computer. Inoltre, si ha la possibilità di effettuare una scansione differenziata in base alle seguenti categorie delle minacce.

- Adware
- Adware/Spyware
- Applicazioni
- Software di controllo backdoor
- File con estensioni nascoste
- Programma di selezione a pagamento
- Phishing
- Programmi che violano la privacy dell'utente
- Programmi ludici
- Giochi
- Software ingannevole
- Strumento di compressione runtime insolito

Facendo clic sulla casella appropriata viene attivata (spuntata) o disattivata (non spuntata) la modalità selezionata.

Attiva tutti

Se l'opzione è attivata vengono attivate tutte le modalità.

Valori predefiniti

Questo pulsante ripristina i valori standard predefiniti.

> **Suggerimenti**
> Se viene disattivata una modalità, i file riconosciuti come tale tipo di programma non verranno più segnalati. Non viene riportata alcuna segnalazione nemmeno sul file di report.

12.8.2 Password

È possibile proteggere il prodotto Avira in diverse sezioni con una password. Se si inserisce una password questa verrà richiesta ogni volta che si desidera aprire una sezione protetta.

Password

Inserimento password

Inserire qui la password desiderata. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*). È possibile inserire un numero massimo di 20 caratteri. Se è stata inserita una password, il programma negherà l'accesso in caso di inserimento di password errata. Un campo vuoto equivale a "Nessuna password".

Conferma

Inserire nuovamente la password per conferma. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

> **Suggerimenti**
> Attenzione alle lettere maiuscole o minuscole!

Aree protette da password (Opzioni disponibili solo in Modalità esperto).

Il prodotto Avira può proteggere singole sezioni con una password. Facendo clic sulla casella appropriata, la richiesta di password per alcune sezioni può essere disattivata o riattivata.

Sezione protetta da password	Funzione
Control Center	Se l'opzione è attivata, per l'avvio del Control Center è necessario inserire la password.
Attiva/disattiva Realtime Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Avira Realtime Protection è necessario inserire la password.
Attiva/disattiva Mail Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Mail Protection è necessario inserire la password.
Attiva/disattiva FireWall	Se l'opzione è attivata, per l'attivazione e la disattivazione del FireWall è necessario inserire la password.
Attiva/disattiva Web Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Web Protection è necessario inserire la password.
Attiva/Disattiva protezione bambini	Se l'opzione è attivata, per l'attivazione e la disattivazione della protezione bambini è necessario inserire la password.
Quarantena	Se l'opzione è attivata, tutte le sezioni del Gestore della quarantena protette da password sono attivate. Facendo clic sulla casella appropriata, la richiesta di password può essere disattivata o riattivata.
Ripristina gli oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per ripristinare un oggetto.
Nuovo controllo di oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per una verifica successiva.
Apri gli oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per visualizzare le proprietà di un oggetto.

Elimina gli oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per eliminare un oggetto.
Invia email ad Avira	Se l'opzione è attivata, è necessario inserire la password per inviare un oggetto al Malware Research Center Avira per una verifica.
Copia di oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per copiare gli oggetti infetti.
Aggiungi e modifica job	Se l'opzione è attivata, per aggiungere e modificare job nello Scheduler, è necessario inserire la password.
Avvio dell'aggiornamento del prodotto.	Se l'opzione è attivata, all'avvio dell'aggiornamento del prodotto nel menu Aggiorna, è necessario inserire la password.
Configurazione	Se l'opzione è attivata, è possibile configurare il programma solo dopo l'inserimento della password.
Installazione / Disinstallazione	Se l'opzione è attivata, per l'installazione e la disinstallazione del programma, è necessario inserire la password.

12.8.3 Sicurezza

Opzioni disponibili solo in Modalità esperto.

Avvio automatico

Blocca avvio automatico

Se l'opzione è attivata, l'avvio automatico di Windows viene bloccato su tutti i drive collegati, come penne USB, CD e DVD, drive di rete. Con la funzione di avvio automatico di Windows, i file sui supporti informatici o sui drive di rete vengono letti immediatamente al momento dell'inserimento o del collegamento; in questo modo i file possono essere avviati e riprodotti automaticamente. Tuttavia questa funzionalità nasconde un rischio per la sicurezza molto elevato, poiché con l'avvio automatico dei file è possibile che vengano installati malware e programmi indesiderati. Particolarmente critica è la funzione di avvio automatico delle penne USB poiché su questi supporti i file possono modificarsi continuamente.

Escludi CD e DVD

Se l'opzione è attivata, è consentita la funzione di avvio automatico sui drive CD e DVD.

Attenzione
Disattivare la funzione di avvio automatico per i drive CD e DVD solo se si è sicuri che si tratti di supporti informatici assolutamente affidabili.

Protezione del sistema

Proteggi il file host di windows da modifiche

Se questa opzione è attivata, i file host di Windows sono protetti dalla scrittura. Non è più possibile manipolare i file. Il malware non è più, ad esempio, in grado di deviare l'utente su pagine Internet indesiderate. Questa opzione è attivata di default.

Tutela del prodotto

Suggerimenti
Le opzioni per la tutela del prodotto non sono disponibili se Realtime Protection non è stato installato in modo personalizzato.

Proteggi i processi da una chiusura indesiderata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata dovuta a virus e malware o a una chiusura involontaria di un utente, ad esempio mediante il Task Manager. Questa opzione è attivata di default.

Protezione del processo avanzata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata con metodi avanzati. La protezione avanzata del processo consuma molte più risorse rispetto alla protezione di processo base. L'opzione è attivata di default. Per disattivare l'opzione è necessario riavviare il computer.

Suggerimenti
Protezione del processo in Windows XP 64 Bitnon disponibile!

Attenzione
Se la protezione del processo è attivata, possono verificarsi problemi di interazione con altri software. In tal caso disattivare la protezione del processo.

Proteggi i file e le voci di registrazione dalla manipolazione

Se l'opzione è attivata, tutte le voci del registro del programma e tutti i dati del programma (file binari e di configurazione) vengono protetti da manipolazione. La protezione da manipolazione comprende la protezione da interventi di scrittura, eliminazione e talvolta di lettura sulle voci del registro o sui file di programma da parte di utenti o di programmi estranei. Per attivare l'opzione è necessario riavviare il computer.

Attenzione
Si noti che, se l'opzione è disattivata, la riparazione dei computer colpiti da alcuni tipi di malware può fallire.

Suggerimenti
Se l'opzione è attivata, è possibile effettuare modifiche della configurazione o di job di scansione e aggiornamento solo tramite l'interfaccia utente.

Suggerimenti
Protezione dei file e delle voci di registrazione in Windows XP 64 Bitnon disponibile!

12.8.4 WMI

Opzioni disponibili solo in Modalità esperto.

Assistenza per Windows Management Instrumentation (WMI)

Windows Management Instrumentation è una tecnologia di gestione fondamentale di Windows che consente, mediante linguaggi di script e di programmazione in lettura e in scrittura, di accedere in locale e in remoto alle impostazioni dei computer Windows. Il prodotto Avira supporta WMI e rende disponibili dati (informazioni sullo stato, statistiche, rapporti, job pianificati ecc.), eventitramite un'interfaccia. Tramite WMI è possibile richiamare dati operativi del programma.

attiva supporto WMI

Se l'opzione è attivata, è possibile richiamare i dati operativi del programma tramite WMI.

12.8.5 Eventi

Opzioni disponibili solo in Modalità esperto.

Limitare l'estensione della banca dati degli eventi

Limita l'estensione ad un massimo di n immissioni

Se l'opzione è attiva, il numero massimo delle immissioni nella banca dati degli eventi è limitato a un preciso numero; i valori consentiti sono: da 100 a 10.000 immissioni. Se il numero delle immissioni viene superato gli inserimenti più vecchi vengono eliminati.

Elimina tutti gli eventi più vecchi di n giorno/i

Se l'opzione è attiva dopo un numero determinato di giorni gli eventi vengono eliminati dalla banca dati degli eventi; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Con l'opzione attivata, le dimensioni della banca dati degli eventi non sono limitate. Sull'interfaccia del programma, alla voce Eventi, viene però visualizzato un massimo di 20.000 immissioni.

12.8.6 Report

Opzioni disponibili solo in Modalità esperto.

Limita i report

Limita il numero a un massimo di n pezzi

Se l'opzione è attiva, il numero massimo di report può essere limitato; i valori consentiti sono: da 1 a 300. Se il numero indicato viene superato, i report più vecchi vengono eliminati.

Elimina tutti i report più vecchi di n giorni

Se l'opzione è attiva i report vengono automaticamente eliminati dopo un determinato numero di giorni; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Se l'opzione è attiva, il numero di report non è limitato.

12.8.7 Directory

Opzioni disponibili solo in Modalità esperto.

Percorso temporaneo

Utilizza le impostazioni predefinite

Se l'opzione è attivata vengono utilizzate le impostazioni del sistema per la gestione dei file temporanei.

Suggerimenti
I file temporanei nel sistema sono memorizzati ad esempio in Windows XP - in: **Start > Impostazioni > Pannello di controllo > Sistema >** Scheda "**Avanzate**" > Pulsanti "**Variabili d'ambiente**". Le variabili temporanee (`TEMP`, `TMP`) per l'utente di volta in volta registrato e per le variabili di sistema (`TEMP`, `TMP`) sono visibili qui con i loro rispettivi valori.

Utilizza la seguente directory

Se l'opzione è attivata viene utilizzato il percorso visualizzato nel campo.

Campo

In questo campo inserire il percorso in cui i file temporanei del programma dovranno essere salvati.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il percorso temporaneo desiderato.

Standard

Il pulsante crea la directory predefinita per il percorso temporaneo.

12.8.8 Avviso acustico

Opzioni disponibili solo in Modalità esperto.

In caso di rilevamento di un virus o di un malware tramite System Scanner o Realtime Protection viene emesso un avviso acustico in modalità di azione interattiva. È possibile attivare o disattivare l'avviso acustico oppure selezionare un file wave alternativo come avviso acustico.

Suggerimenti
La modalità di azione di System Scanner viene impostata nella configurazione in **System Scanner > Scansione > Azione in caso di rilevamento**. La modalità di azione di Realtime Protection viene impostata nella configurazione in **Realtime Protection > Scansione > Azione in caso di rilevamento**.

Nessun avviso

Se l'opzione è attivata, non viene emesso alcun avviso acustico in caso di rilevamento tramite System Scanner o Realtime Protection.

Emetti tramite casse PC (solo in modalità interattiva)

Se l'opzione è attivata, viene emesso un avviso acustico con suono standard in caso di rilevamento di un virus tramite System Scanner o Realtime Protection. L'avviso acustico viene emesso tramite l'altoparlante interno del PC.

Utilizza il seguente file WAVE (solo in modalità interattiva)

Se l'opzione è attivata, in caso di rilevamento di un virus tramite System Scanner o Realtime Protection viene emesso un avviso acustico con il file wave selezionato. Il file wave selezionato viene riprodotto tramite un altoparlante collegato esternamente.

File wave

In questo campo è possibile inserire il nome e il percorso corrispondente di un file audio. L'avviso acustico standard del programma viene immesso di default.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file desiderato grazie all'explorer dei file.

Test

Questo pulsante serve a testare il file wave selezionato.

12.8.9 Avvisi

Il prodotto Avira, in caso di determinati eventi, genera messaggi sul desktop, i cosiddetti messaggi a tendina, per informare l'utente di eventuali pericoli o della riuscita o meno dell'esecuzione di un dato programma come, per esempio, un aggiornamento. È possibile attivare o disattivare in **Avvisi** la funzione di notifica per specifici eventi.

Nel caso delle notifiche sul desktop è possibile disattivare direttamente le notifiche sul messaggio a tendina. È possibile annullare la disattivazione della notifica nella finestra di configurazione **Avvisi**.

Aggiornamento

Avviso se l'aggiornamento risale a più di n giorni fa

In questo campo, è possibile inserire il numero massimo di giorni che possono trascorrere dall'ultimo aggiornamento. Se si supera questo periodo, il Control Center visualizzerà sotto Stato un'icona rossa per lo stato dell'aggiornamento.

Avvisa se il file VDF non è aggiornato

Se l'opzione è attivata, si riceve un avviso in caso di file di definizione dei virus non aggiornato. Grazie all'opzione "Avviso, se l'ultimo aggiornamento risale a più di n giorni fa", è possibile configurare un intervallo temporale.

Avvisi/indicazione nelle seguenti situazioni

Utilizzo di una connessione dial-up

Se l'opzione è attivata, l'utente è avvisato con una notifica sul desktop quando un programma di selezione stabilisce una connessione sul computer tramite la rete telefonica o ISDN. In caso di programmi di selezione esiste il rischio che si tratti di un dialer sconosciuto e indesiderato, che stabilisce una connessione a pagamento. (vedere Categorie di minacce: Dialer)

File aggiornati correttamente

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato completato con successo un aggiornamento e sono stati aggiornati file.

Aggiornamento non riuscito

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando un aggiornamento non è stato completato con successo: Non è stato possibile stabilire una connessione con il server di download o non è stato possibile installare i file aggiornati.

Non sono necessari aggiornamenti

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato lanciato un aggiornamento ma non era necessario installare alcun file perché il programma era già aggiornato.